4.8.5 Personal Use of Government Office Equipment and DHS Systems/Computers

Policy ID	DHS Policy Statements	Relevant Controls
4.8.5.a	DHS employees may use Government office equipment and DHS systems/computers for authorized purposes only. "Authorized use" includes limited personal use as described in DHS MD 4600.1, *Personal Use of Government Office Equipment*, and DHS MD 4900, *Individual Use and Operation of DHS Information Systems/Computers*.	---
4.8.5.b	Limited personal use of DHS email and Internet services is authorized for DHS employees as long as this use does not interfere with official duties, inhibit the security of information and information systems, or cause degradation of network services. Specifically prohibited activities include streaming of audio or video, social networking, peer-to-peer networking, software or music sharing/piracy, online gaming, webmail, Instant Messaging (IM), hacking, and the viewing of pornography or other offensive content. DHS users shall comply with the provisions of DHS MD 4500.1, *DHS E-mail Usage*, and DHS MD 4400.1, *DHS Web and Information Systems*.	---
4.8.5.c	Anyone granted user account access to any DHS information system (including DHS employees, contractors, and others working on behalf of DHS) shall have no expectations of privacy associated with its use. By completing the authentication process, the user acknowledges his or her consent to monitoring.	AC-8
4.8.5.d	The use of Government office equipment and DHS systems/computers constitutes consent to monitoring and auditing of the equipment/systems at all times. Monitoring includes the tracking of internal transactions and external transactions such as Internet access. It also includes auditing of stored data on local and network storage devices as well as removable media.	AC-8
4.8.5.e	DHS users are required to sign rules of behavior prior to being granted system accounts or access to DHS systems or data. The rules of behavior shall contain a "Consent to Monitor" provision and an acknowledgement that the user has no expectation of privacy.	PL-4
4.8.5.f	Contractors, others working on behalf of DHS, or other non-DHS employees are not authorized to use Government office equipment or information systems/computers for personal use, unless limited personal use is specifically permitted by the contract or memorandum of agreement. When so authorized, the limited personal use policies of this section and the provisions of DHS MD 4600.1, DHS MD 4900, DHS MD 4400.1, and DHS MD 4500.1 shall apply.	---

4.8.6 Wireless Settings for Peripheral Equipment

Peripheral equipment (printers, scanners, fax machines) often includes capabilities, intended to allow wireless access to these devices. Although convenient, wireless access comes with additional risks. In general, wireless access is not allowed on DHS networks.

Policy ID	DHS Policy Statements	Relevant Controls
4.8.6.a	Components shall ensure that wireless capabilities for peripheral equipment are disabled. This applies all to peripherals connected to any DHS network or to systems processing or hosting DHS sensitive data.	CM-7
4.8.6.b	In cases where valid mission requirements or equipment limitations prevent disabling wireless capabilities, Components shall comply with all requirements outlined in Section 4.6, Wireless Communication *and* obtain a waiver or exception in accordance with this policy.	CM-7

4.9 Department Information Security Operations

The DHS EOC is the central coordinating and reporting authority for all Sensitive and National Security computer security incidents throughout the Department. The HSDN SOC shall report incidents to the DHS EOC through appropriate channels to protect data classification. The HSDN SOC is subordinate to the DHS EOC, acting as the central coordinating and reporting authority for all SECRET computer security incidents throughout the Department.

Policy ID	DHS Policy Statements	Relevant Controls
4.9.a	It is the policy of DHS that employees, contractors, or others working on behalf of DHS have no privacy expectations associated with the use of any DHS network, system, or application. This policy is further extended to anyone who is granted account access to any network, system, or application in use in the Department. By completing the account log in process the account owner acknowledges their consent to monitoring.	AC-8, PL-4
4.9.b	Component SOCs and the HSDN SOC shall be operationally subordinate to the DHS EOC. The DHS EOC shall provide operational oversight and guidance.	IR-1
4.9.c	The DHS EOC or Component SOCs shall lead the coordination and administration of Department and Component policy enforcement points, such as firewalls.	SC-7
4.9.d	The DHS EOC shall implement the Department logging strategy, coordinated with Component SOCs, to enable endpoint visibility and Departmental situational awareness.	---
4.9.e	All SOCs shall have the capability to process intelligence information at the collateral level or above. The DHS EOC and Component SOCs shall have the ability to process SECRET level information continuously and shall have the capability to receive TS/SCI information.	IR-4
4.9.f	SOCs shall ensure that personnel are appropriately cleared to access Joint Worldwide Intelligence Communications System (JWICS). SOC managers are free to determine the number and type of personnel to be cleared, but at least	IR-4

Policy ID	DHS Policy Statements	Relevant Controls
	one cleared person shall be available per shift. (This person may be on call.) A Government officer shall be available continuously for incident response and management.	
4.9.g	All Department SOCs shall establish and maintain a forensic capability as outlined in the DHS Enterprise Operations Concept of Operations (EOC CONOPS).	IR-7
4.9.h	Department information security operations shall provide a vulnerability management capability. DHS EOC provides Information Security Vulnerability Management (ISVM) messages and vulnerability assessment capabilities. Component SOCs shall develop a robust vulnerability management capability to compliment the DHS EOC.	SI-5
4.9.i	Component CISOs shall ensure that the DHS CISO is kept apprised of all pertinent matters involving the security of information systems and that security-related decisions and information are distributed to the ISSOs and other appropriate persons.	SI-5
4.9.j	Component SOCs shall report operationally to the respective Component CISO. Each CISO shall exercise oversight over their Components' information security operations functions, including the Component SOCs.	IR-1
4.9.k	The DHS EOC shall report operationally to the DHS CISO.	

4.10 Security Incidents and Incident Response and Reporting

Policy ID	DHS Policy Statements	Relevant Controls
4.10.a	Components shall establish and maintain a continuous incident response capability.	IR-1
4.10.b	Components shall report *significant incidents* to the DHS EOC by calling (703) 921-6505 as soon as possible but not later than one (1) hour from "validation" (e.g., a security event being confirmed as a security incident). Other means, such as the EOC ONLINE portal (https://eoconline.dhs.gov) are acceptable, but the Component shall positively verify that the notification is received and acknowledged by the DHS EOC.	IR-6
4.10.c	Significant HSDN incidents shall be documented with a preliminary report that shall be provided to the HSDN Government Watch Officer or DHS EOC within one hour. An initial detailed report shall be provided to the DHS EOC as soon as possible but not later than one hour from "validation" via secure communications. Subsequent updates and status reports shall be provided to the DHS EOC every twenty-four (24) hours via HSDN SOC ONLINE until incident resolution or when new information is discovered. Significant	IR-6

Policy ID	DHS Policy Statements	Relevant Controls
	incidents are reported individually on a per incident basis and shall not be reported in the monthly summary report. Additional guidance is located in DHS 4300A Attachment F, *Incident Response and Reporting,* Section 3.0.	
4.10.d	Components shall report minor incidents on systems in the weekly incident report. SBU systems may report via the DHS EOC portal (https://eoconline.dhs.gov). Components with no portal access shall report minor incidents via email to dhs.soc@dhs.gov. HSDN incidents or incidents involving SECRET information shall be documented in a summary report via the HSDN DHS EOC portal.	IR-6
4.10.e	DHS personnel shall follow DHS CISO procedures for detecting, reporting, and responding to information security incidents in accordance with the DHS EOC CONOPS. Reports shall be classified at the highest classification level of the information contained in the document. Unsanitized reports shall be marked and handled appropriately.	IR-1
4.10.f	If a DHS Component has no incidents to report for a given week, a weekly "No Incidents" report shall be sent to the EOC.	IR-6
4.10.g	The DHS EOC shall report incidents to US-CERT, in accordance with the DHS EOC CONOPS. Components shall not send incident reports directly to US-CERT.	IR-6
4.10.h	The DHS EOC shall receive classified spillage incident reports, and support the DHS CSO for containment and cleanup. All classified spillages are significant incidents.	IR-6
4.10.i	The DHS EOC shall maintain information security "playbooks," that is, checklists that implement procedures and provide guidance on how to respond rapidly to developing incidents.	IR-1
4.10.j	The DHS EOC shall respond to detected faults, attacks, events, or incidents and communicate incident reports to external organizations that may be affected.	IR-1
4.10.k	Components shall maintain a full SOC and CSIRC capability or outsource this capability to the DHS EOC. The DHS EOC shall provide SOC and CSIRC services to Components in accordance with formal agreements. Information regarding incident response capability is available in Attachment F of the DHS 4300A *Sensitive Systems Handbook.*	IR-7
4.10.l	Components shall develop and publish internal computer security incident response plans and incident handling procedures, and provide copies to the DHS CSIRC. These procedures shall include a detailed CM process for modification of security device configurations.	IR-1

Policy ID	DHS Policy Statements	Relevant Controls
4.10.m	Component Heads shall take corrective actions when security incidents and violations occur and shall hold personnel accountable for intentional transgressions.	IR-1
4.10.n	The DHS EOC shall monitor and report incident investigation and incident remediation activities to the DHS CIO and CISO in accordance with the DHS EOC CONOPS until the incident is closed.	IR-5
4.10.o	The DHS CISO shall determine the frequency and content of security incident reports.	IR-6
4.10.p	The Component CSIRC shall report incidents only to the DHS EOC and to no other external agency or organization.	IR-6
4.10.q	The DHS CISO shall publish Incident Response Testing and Exercise scenarios as required.	IR-1
4.10.r	The Component CISO for each Component providing an incident response capability shall ensure Incident Response Testing and Exercises are conducted annually in coordination with the DHS CISO.	IR-3

4.10.1 Law Enforcement Incident Response

The DHS EOC shall notify the DHS Chief, Internal Security and Investigations Division, Office of Security (CISID-OIS) whenever an incident requires law enforcement involvement. Law enforcement shall coordinate with the DHS EOC, the CISID-OIS, the Component, and other appropriate parties whenever a crime is committed or suspected.

Policy ID	DHS Policy Statements	Relevant Controls
4.10.1.a	Components shall coordinate all external law enforcement involvements through the DHS EOC and obtain guidance from the DHS EOC before contacting local law enforcement. Exceptions are only made during emergencies where there is risk to life, limb, or destruction of property. In cases of emergency notification, the Component shall notify the DHS EOC as soon as possible, by the most expedient means available.	IR-6
4.10.1.b	Security Incidents may include law enforcement (LE) or counter intelligence (CI) elements, such as maintaining a chain of custody. All incidents containing a LE/CI aspect shall be coordinated with the DHS CSO through the DHS EOC.	IR-6

4.11 Documentation

Policy ID	DHS Policy Statements	Relevant Controls
4.11.a	Components shall ensure that information systems and networks are appropriately documented in such a way as to allow others to understand system operation and configuration.	CM-8
4.11.b	System Owners shall update system documentation annually or whenever system changes occur. Such changes include: • A vulnerability scan of the information system; • New threat information; • Weaknesses or deficiencies discovered in currently deployed security controls after an information system breach; • A redefinition of mission priorities or business objectives resulting in a change to the security category of the information system; and A change in the information system (e.g., adding new hardware, software, or firmware; establishing new connections) or the system's environment of operation	CM-3, CM-8, SA-5
4.11.c	Documentation shall be kept on hand and be accessible to authorized personnel (including auditors) at all times.	CM-3
4.11.d	System documentation may be categorized as Sensitive if deemed appropriate by the Component CISO/ISSM. This category shall not be used as a means to restrict access to auditors or other authorized personnel.	CM-3

4.12 Information and Data Backup

Policy ID	DHS Policy Statements	Relevant Controls
4.12.a	The policies in this document, including Security Authorization Process requirements, apply to any devices that process or host DHS data.	---
4.12.b	Component CISOs/ISSMs shall determine whether or not automated process devices shall be included as part of an information system's Security Authorization Process requirements.	---
4.12.c	. This policy directive and the DHS 4300A Sensitive Systems Handbook apply to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS data. This includes prototypes, telecommunications systems, and all systems in all phases of the System Engineering Life Cycle.	---

4.13 Converging Technologies

Advances in technology have resulted in the availability of devices that offer multiple functions. Many devices such as multifunctional desktop computers, copiers, facsimile machines, and heating, ventilation and air conditioning (HVAC) systems may contain sensitive data and may also be connected to data communications networks.

Policy ID	DHS Policy Statements	Relevant Controls
4.13.a	The policies in this document apply to any networked devices that contain information technology, including copiers, facsimile machines, and alarm control systems.	---
4.13.b	Components shall ensure that network printers and facsimile machines are updated to the latest version of their firmware/software at least annually.	CM-2
4.13.c	Components shall ensure that network printers, copiers, and facsimile machines shall be configured for least required functionality.	CM-7
4.13.d	Components shall ensure that each network printer, copier, and facsimile machine is within the system definition of a DHS information system that has a current ATO.	CM-8
4.13.e	Components shall ensure that remote maintenance of network printers, copiers, and facsimile machines is conducted only from within DHS networks. If maintenance planning does not include performing remote maintenance, Components shall ensure that remote maintenance capabilities are disabled.	MA-4
4.13.f	Components shall ensure that network printers, copiers, and facsimile machines are configured to restrict administrator access to authorized individuals or groups.	MA-5
4.13.g	Components shall ensure that maintenance or disposal of network printers, copiers, or facsimile machines, approved for sensitive reproduction, is performed only while escorted by a properly cleared person with knowledge to detect any inappropriate action.	MA-5
4.13.h	Components shall ensure that memory and hard drives do not leave the facility; they are to be replaced and the old part destroyed as sensitive media.	MP-6
4.13.i	Components shall locate network printers, copiers, and facsimile machines approved to process sensitive information in areas where access can be controlled when paper output is being created.	PE-18
4.13.j	Any multifunction device connected to a DHS network or other information system containing sensitive data shall have the inbound dial in capabilities disabled.	AC-17

5.0 TECHNICAL POLICIES

The design of information systems that process, store, or transmit sensitive information shall include the automated security features discussed in this section. Security safeguards shall be in place to ensure that each person having access to sensitive information systems is individually accountable for his or her actions while utilizing the system.

5.1 Identification and Authentication

Policy ID	DHS Policy Statements	Relevant Controls
5.1.a	Components shall ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.	IA-1, IA-2
5.1.b	For information systems requiring authentication controls, Components shall ensure that the information system is configured to require that each user be authenticated before information system access occurs.	IA-1, IA-2
5.1.c	For systems with low impact for the confidentiality security objective, Components shall disable user identifiers after ninety (90) days of inactivity; for systems with moderate and high impacts for the confidentiality security objective, Components shall disable user identifiers after forty-five (45) days of inactivity.	IA-4
5.1.d	DHS users shall not share identification or authentication materials of any kind, nor shall any DHS user allow any other person to operate any DHS system by employing the user's identity.	IA-5
5.1.e	All user authentication materials shall be treated as sensitive material and shall carry a classification as high as the most sensitive data to which that user is granted access using that authenticator.	IA-7
5.1.f	Components shall implement strong authentication on servers, for system administrators and personnel with significant security responsibilities, within six (6) months of the Component's implementation of Homeland Security Presidential Directive (HSPD) HSPD-12.	IA-2

5.1.1 Passwords

The least expensive method for authenticating users is a password system in which authentication is performed each time a password is used. More sophisticated authentication techniques, such as Smart Cards and biological recognition systems (e.g., retina scanner, handprint, voice recognition), shall be cost-justified through the risk assessment process.

Policy ID	DHS Policy Statements	Relevant Controls
5.1.1.a	In those systems where user identity is authenticated by password, the system ISSO shall determine and enforce appropriate measures to ensure that strong passwords are used.	IA-5
5.1.1.b	The ISSO shall determine and enforce the appropriate frequency for changing passwords in accordance with appropriate guidance documentation (if published). In the absence of specific guidance documentation, passwords shall not remain in effect longer than ninety (90) days.	IA-5
5.1.1.c	DHS users shall not share personal passwords.	IA-5
5.1.1.d	Use of group passwords is limited to situations dictated by operational necessity or critical for mission accomplishment. Use of a group User ID and password shall be approved by the appropriate AO.	IA-4
5.1.1.e	Components shall prohibit passwords from being embedded in scripts or source code.	IA-5
5.1.1.f	Components shall ensure that all passwords are stored in encrypted form.	IA-5

The use of a personal password by more than one individual is prohibited throughout the DHS. However, it is recognized that, in certain circumstances such as the operation of crisis management or operations centers, watch team, and other duty personnel may require the use of group User IDs and passwords.

5.2 Access Control

Policy ID	DHS Policy Statements	Relevant Controls
5.2.a	Components shall implement access control policy and procedures that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.	AC-1
5.2.b	Access control shall follow the principles of least privilege and separation of duties and shall require users to use unique identifiers. *Social Security Numbers shall not be used as login IDs.*	AC-2, IA-1
5.2.c	Users shall not provide their passwords to anyone, including system administrators.	IA-5
5.2.d	Emergency and temporary access authorization shall be strictly controlled and shall be approved by the Component CISO/ISSM or his/her designee prior to being granted.	AC-2

Policy ID	DHS Policy Statements	Relevant Controls
5.2.e	System Owners shall ensure that users are assigned unique account identifiers.	AC-2, IA-4
5.2.f	DHS systems with a FIPS 199 confidentiality categorization of high shall limit the number of concurrent sessions for any user to one (1).	AC-10

5.2.1 Automatic Account Lockout

Components shall configure each information system to lock a user's account for a specified period following a specified number of consecutive failed logon attempts. Users shall be locked from their account for a period of twenty (20) minutes after three consecutive failed logon attempts during a twenty-four (24) hour time period. All failed logon attempts must be recorded in an audit log and periodically reviewed.

Policy ID	DHS Policy Statements	Relevant Controls
5.2.1.a	Components shall configure accounts to automatically lock a user's *account* after three consecutive failed logon attempts during a twenty-four (24) hour time period.	AC-7
5.2.1.b	The automatic lockout period for accounts locked due to failed login attempts shall be set for twenty (20) minutes.	AC-7
5.2.1.c	Components shall establish a process for manually unlocking accounts prior to the expiration of the twenty (20) minute period, after sufficient user identification is established. This may be accomplished through the help desk.	AC-7

5.2.2 Automatic Session Termination

A session refers to a connection between a terminal device (workstation, laptop, PED) and a networked application or system. (This does not include a direct connection to a DHS network, such as authenticating from a device that is directly connected to a DHS network.) A session also refers to accessing an application or system through the DHS network, such as a database or networked application. When a session is locked, the user may resume activity by reauthenticating. When a session is terminated, the user is disconnected and all unsaved work is lost.

Policy ID	DHS Policy Statements	Relevant Controls
5.2.2.a	Components shall configure networked applications or systems to automatically lock any user session in accordance with the appropriate configuration guide. In the absence of configuration guidance, the session shall lock following twenty (20) minutes of inactivity.	AC-11

Policy ID	DHS Policy Statements	Relevant Controls
5.2.2.b	Locked sessions shall remain locked until the user re-authenticates.	AC-11
5.2.2.c	Sessions shall automatically be terminated after sixty (60) minutes of inactivity.	SC-10

5.2.3 Warning Banner

The DHS CISO stipulates that a warning banner statement be displayed on all DHS systems during logon. The most current language can be found on the DHS CISO web page.

Please note that the current warning banner was developed specifically for use on DHS workstations. Due to differing function, purpose and situation as well as length requirements, warning banners for other environments, such as routers, switches and public-facing websites, will be developed and included in a future version of the DHS 4300A *Sensitive Systems Handbook*.

The use of the warning banner serves as a reminder to all users that the computers they are accessing are Government computers.

Policy ID	DHS Policy Statements	Relevant Controls
5.2.3.a	Systems internal to the DHS network shall display a warning banner stipulated by the DHS CISO.	AC-8
5.2.3.b	Systems accessible to the public shall provide both a security and privacy statement at every entry point.	AC-8

5.3 Auditing

Policy ID	DHS Policy Statements	Relevant Controls
5.3.a	Audit records shall be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Audit records shall be reviewed as specified in the SP. The audit record shall contain at least the following information: - Identity of each user and device accessing or attempting to access the system - Time and date of the access and the logoff - Activities that might modify, bypass, or negate information security safeguards - Security-relevant actions associated with processing - All activities performed using an administrator's identity	AU-3
5.3.b	Audit records for financial systems or for systems hosting or processing PII shall be reviewed each month. Unusual activity or unexplained access attempts shall be reported to the System Owner and Component CISO/ISSM.	AU-6
5.3.c	Components shall ensure that their audit records and audit logs are protected from unauthorized modification, access, or destruction.	AU-9
5.3.d	Components shall ensure that audit logs are recorded and retained in accordance with the Component's Record Schedule or the DHS Records Schedule. At a minimum audit trail records shall be maintained *online* for at least ninety (90) days. *Audit trail records shall be preserved for a period of seven (7) years* as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease.	AU-11
5.3.e	Components shall evaluate the system risks associated with extracts of PII from databases. If the risk is determined to be sufficiently high, a procedure shall be developed for logging computer-readable data extracts. If logging these extracts is not possible, this determination shall be documented, and compensating controls identified in the SP.	AU-1, AU-2, AU-3, PM-9
5.3.f	Component SOCs shall implement both general and threat-specific logging.	AU-1

5.4 Network and Communications Security

5.4.1 Remote Access and Dial-In

Remote access technology allows trusted employees to access DHS networks by dialing in via modem or accessing the DHS network via the Internet. This allows mobile employees to stay in touch with the home office while traveling away from their normal work locations. However, there are significant security risks associated with remote access and dial-in capabilities. Proper procedures can help mitigate these risks.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.1.a	Data communication connections via modems shall be limited and shall be tightly controlled as such connections can be used to circumvent security controls intended to protect DHS networks. Data communication connections are not allowed unless they have been authorized by the Component CISO/ISSM. Approved remote access to DHS networks shall only be accomplished through equipment specifically approved for that purpose. Tethering through wireless PEDs is prohibited unless approved by the appropriate AO.	AC-4, AC-17, AU-2 SC-7, SC-8, SC-9
5.4.1.b	Components shall centrally manage all remote access and dial-in connections to their systems and shall ensure that remote access and approved dial-in capabilities provide strong authentication, two-factor authentication, audit capabilities, and protection for sensitive information throughout transmission. DHS has an immediate goal that remote access shall only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Any two-factor authentication shall be based on Department-controlled certificates or hardware tokens issued directly to each authorized user. Remote access solutions shall comply with the encryption requirements of FIPS 140-2, *Security Requirements for Cryptographic Modules*. See Privacy Controls Section (Section 3.14) for additional requirements involving remote access of PII.	AC-4, AC-17, AU-2 SC-7, SC-8, SC-9
5.4.1.c	Remote access of PII shall comply with all DHS requirements for sensitive systems, including strong authentication. Strong authentication shall be accomplished via virtual private network (VPN) or equivalent encryption and two-factor authentication. The Risk Assessment and SP shall document any remote access of PII, and the remote access shall be approved by the AO prior to implementation.	AC-4, AC-17, AU-2 SC-7, SC-8, SC-9
5.4.1.d	Remote access of PII shall not permit the download and remote storage of information unless the requirements for the use of removable media with sensitive information have been addressed. All downloads shall follow the concept of least privilege and shall be documented with the SP.	---

5.4.2 Network Security Monitoring

Security Monitoring, Detection and Analysis are key functions and are critical to maintaining the security of DHS information systems. Monitoring and analysis is limited to observing network activity for anomalies, malicious activities and threat profiles. Content analysis is not within the scope of network monitoring.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.2.a	Components shall provide continuous monitoring of their networks for security events or outsource this requirement to the DHS EOC. Monitoring includes interception and disclosure as required for the rendition of service or to protect the Department's or Component's rights or property. Service observing or random monitoring shall not be used except for mechanical or service quality control checks. (As per the Electronic Communications Privacy Act) In this instance, "rights" refers to ownership or entitlements or property or information as in intellectual property.	SI-4
5.4.2.b	The DHS EOC shall administer and monitor DHS intrusion detection system (IDS) sensors and security devices.	SI-4
5.4.2.c	Component SOCs shall administer and monitor Component IDS sensors and security devices.	SI-4

5.4.3 Network Connectivity

A system interconnection is the direct connection of two or more information systems for the purpose of sharing data and other information resources. This applies to systems that pass data between each other via a direct system-to-system interface without human intervention. Any physical connection that allows other systems to share data (pass thru) also constitutes an interconnection, even if the two systems connected do not share data between them. It does not include instances of a user logging on to add or retrieve data, nor users accessing web-enabled applications through a browser.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.3.a	Components shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network element.	AC-1, AC-2, AU-1, AU-2, IA-1, IA-2
5.4.3.b	Interconnections between DHS and non-DHS systems shall be established only through controlled interfaces and via approved service providers. The controlled interfaces shall be accredited at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memoranda of understanding, service level agreements or interconnection security agreements.	CA-3
5.4.3.c	Components shall document all interconnections to the DHS OneNet with an ISA, signed by the OneNet AO and by each applicable AO. Additional information regarding ISAs is published in Attachment N, *Preparation of Interconnection Security Agreements*, to the DHS 4300A *Sensitive Systems*	CA-3

Policy ID	DHS Policy Statements	Relevant Controls
	Handbook.	
5.4.3.d	ISAs shall be reissued every three (3) years or whenever any significant changes have been made to any of the interconnected systems.	CA-3
5.4.3.e	ISAs shall be reviewed and updated as needed as a part of the annual FISMA self-assessment.	CA-3
5.4.3.f	Components may complete a master ISA, (which includes all transitioning systems) as part of their initial OneNet transition. After transition, each additional system or GSS shall be required to have a separate ISA. Interconnections between DHS Components (not including DHS OneNet) shall require an ISA whenever there is a difference in the security categorizations for confidentiality, integrity, and availability between the systems or when the systems do not share the same security policies. (In this context, 'security policies' refers to the set of rules that controls a system's working environment and not to DHS information security policy.) ISAs shall be signed by each applicable AO.	---
5.4.3.g	Components shall document interconnections between their own and external (Non-DHS) networks with an ISA for each connection.	CA-3
5.4.3.h	The DHS CIO shall approve all interconnections between DHS enterprise-level information systems and non-DHS information systems. The DHS CIO shall ensure that connections with other Federal Government Agencies are properly documented. A single ISA may be used for multiple connections provided that the security accreditation is the same for all connections covered by that ISA.	CA-3
5.4.3.i	The Department and Components shall implement Trust Zones through Policy Enforcement Points (PEP), as defined in the DHS Security Architecture.	SC-7
5.4.3.j	DHS OneNet shall provide secure Name/Address resolution service. Domain Name System Security Extensions (DNSSEC) has been designated as the DHS service solution.	SC-20, SC-21, SC-22
5.4.3.k	All DHS systems connected to OneNet and operating at moderate or high level shall utilize secure Name/Address resolution service provided by DHS OneNet.	SC-20, SC-21, SC-22
5.4.3.l	The appropriate CCB shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline. DHS systems that interface with OneNet shall also be subject to the OneNet CCB.	CM-3

Policy ID	DHS Policy Statements	Relevant Controls
5.4.3.m	Interconnections between two accredited DHS systems do not require an ISA if the interface characteristics, security requirements, nature of information communicated and monitoring procedures for verifying enforcement of security requirements are accounted for in the SPs or are described in another formal document, such as a Service Level Agreement (SLA) or contract, and the risks have been assessed and accepted by all involved AOs.	CA-3
5.4.3.n	Granting the ability to log into one DHS system through another DHS system (such as through OneNet trust) does not require an ISA, when the requirements from Section 5.4.3.m are met.	---

5.4.4 Firewalls and Policy Enforcement Points

Policy Enforcement Points (PEP) separate Trust Zones as defined in the DHS Security Architecture. Boundary protection between DHS and external networks is implemented by firewalls at the TICs and other approved direct system inter-connections. DHS TICs are provided by OneNet and monitored by the DHS EOC. Component SOCs may protect DHS-internal boundaries across Trust Zones.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.4.a	Components shall restrict physical access to firewalls and PEP to authorized personnel.	AC-4, SC-7
5.4.4.b	Components shall implement identification and strong authentication for administration of the firewalls and PEPs.	AC-4, SC-7
5.4.4.c	Components shall encrypt remote maintenance paths to the firewalls and PEPs.	MA-4, SC-7
5.4.4.d	Components shall conduct quarterly firewall and PEP testing to ensure that the most recent policy changes have been implemented and that *all* applied policies and controls are operating as intended.	SC-7
5.4.4.e	Component SOCs shall ensure that reports on information security operations status and incident reporting are provided to the DHS CISO as required.	IR-6
5.4.4.f	All Department and Component firewalls and PEPs shall be administered in coordination with DHS security operation capabilities, through the DHS EOC or Component SOCs.	SC-7
5.4.4.g	All DHS PEPs shall provide protection against denial-of-service attacks.	SC-5

Policy ID	DHS Policy Statements	Relevant Controls
5.4.4.h	Components shall determine protocols and services permitted through their Component-level PEPs. Components may restrict traffic sources and destinations at their Component-level PEPs.	SC-7
5.4.4.i	The DHS CISO shall establish policy to block or allow traffic sources and destinations at the DHS TIC PEPs. The DHS CISO policy shall prevent traffic as directed by the DHS CIO.	SC-7
5.4.4.j	The DHS EOC shall oversee all enterprise PEPs.	---

5.4.5 Internet Security

Policy ID	DHS Policy Statements	Relevant Controls
5.4.5.a	Any direct connection of OneNet, DHS networks, or DHS mission systems to the Internet or to extranets shall occur through DHS TIC PEPs. The PSTN shall not be connected to OneNet at any time.	SC-7
5.4.5.b	Firewalls and PEPs shall be configured to prohibit any protocol or service that is not explicitly permitted.	CM-7, SC-7, SC-8, SC-9
5.4.5.c	Components shall ensure that all executable code, including mobile code (e.g., ActiveX, JavaScript), is reviewed and approved by the Program Manager prior to the code being allowed to execute within the DHS environment. [Note: When the technology becomes available and code can be vetted for security, the policy will be "Ensure that all approved code, including mobile code (e.g., ActiveX, JavaScript), is digitally signed by the designated DHS authority and that only signed code is allowed to execute on DHS systems."]	SC-18
5.4.5.d	Telnet shall not be used to connect to any DHS computer. A connection protocol such as Secure Shell (SSH) that employs secure authentication (two factor, encrypted, key exchange) and is approved by the Component shall be used instead.	CM-7, SC-7, SC-8, SC-9
5.4.5.e	File Transfer Protocol (FTP) shall not be used to connect to or from any DHS computer. A connection protocol that employs secure authentication (two factor, encrypted, key exchange) and is approved by the Component shall be used instead.	CM-7, SC-7, SC-8, SC-9
5.4.5.f	Remote Desktop connections, such as Microsoft's Remote Desktop Protocol (RDP), shall not be used to connect to or from any DHS computer without the use of an authentication method that employs secure authentication (two-factor, encrypted, key exchange).	AC-17, IA-2

Policy ID	DHS Policy Statements	Relevant Controls
5.4.5.g	In order to ensure the security and availability of DHS information and information systems, the DHS CIO or DHS CISO may direct that specific Internet websites or categories be blocked at the DHS TICs, on advice from US-CERT, the DHS EOC, or other reputable sources.	---

5.4.6 Email Security

The DHS email gateway Steward provides email monitoring for spam and virus activity at the gateway.

DHS EOC personnel shall be trained to respond to incidents pertaining to email security and shall assist the email Steward as necessary. Components shall provide appropriate security for their email systems.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.6.a	Components shall correctly secure, install, and configure the underlying email operating system.	---
5.4.6.b	Components shall correctly secure, install, and configure mail server software.	---
5.4.6.c	Components shall secure and filter email content.	---
5.4.6.d	Components shall deploy appropriate network protection mechanisms, such as: - Firewalls - Routers - Switches - Intrusion detection systems	---
5.4.6.e	Components shall secure mail clients.	---
5.4.6.f	Components shall conduct mail server administration in a secure manner. This includes: - Performing regular backups - Performing periodic security testing - Updating and patching software - Reviewing audit logs at least weekly	---
5.4.6.g	The DHS email gateway Steward shall provide email monitoring for malware activity at the gateway.	SI-3
5.4.6.h	The DHS email gateway Steward shall provide email monitoring for spam at the gateway.	SI-8

Policy ID	DHS Policy Statements	Relevant Controls
5.4.6.i	Auto-forwarding or redirecting of DHS email to address outside of the .gov or .mil domain is prohibited and shall not be used. Users may manually forward individual messages after determining that the risk or consequences are low.	---
5.4.6.j	All DHS email systems are required to use the common naming convention with distinguishing identifiers for military officers, contractors, foreign nationals, and U.S. Government personnel from other Departments and agencies.	---

Note: Due to the significant risk associated with HTML email, DHS is considering following the lead of the Department of Defense (DoD) and moving to text based email.

5.4.7 Personal Email Accounts

Policy ID	DHS Policy Statements	Relevant Controls
5.4.7.a	The use of Internet webmail (Gmail, Yahoo, AOL) or other personal email accounts is not authorized over DHS furnished equipment or network connections.	---
5.4.7.b	When sending email to an address outside of the .gov or .mil domain, users shall ensure that any sensitive information, particularly PII, is attached as an encrypted file.	---

5.4.8 Testing and Vulnerability Management

The DHS EOC takes a proactive approach to vulnerability management including detecting vulnerabilities through testing, reporting through ISVM messages, and conducting Vulnerability Assessments (VA).

Vulnerability management is a combination of detection, assessment, and mitigation of weaknesses within a system. Vulnerabilities may be identified from a number of sources, including reviews of previous risk assessments, audit reports, vulnerability lists, security advisories, and system security testing such as automated vulnerability scanning or security assessments.

Core elements of vulnerability management include continuous monitoring and mitigating the discovered vulnerabilities, based on a risk management strategy. This strategy accounts for vulnerability severity, threats, and assets at risk.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.8.a	Components shall conduct vulnerability assessments and/or testing to identify security vulnerabilities on information systems containing sensitive information annually or whenever significant changes are made to the information systems. This shall include scanning for unauthorized wireless	---

Policy ID	DHS Policy Statements	Relevant Controls
	devices. Evidence that annual assessments have been conducted shall be included in SARs and with annual security control assessments.	
5.4.8.b	Component CISOs/ISSMs shall approve and manage all activities relating to requests for Vulnerability Assessment Team (VAT) assistance in support of incidents, internal and external assessments, and on-going SLC support.	---
5.4.8.c	Component CISOs/ISSMs or their designated representatives shall acknowledge receipt of ISVM messages.	SI-5
5.4.8.d	Components shall report compliance with the ISVM message within the specified timeframe. Components unable to meet the designated compliance timeframe shall submit documentation of a waiver request via the DHS EOC Online Portal (https://eoconline.dhs.gov).	SI-5
5.4.8.e	When vulnerability assessment responsibilities encompass more than one Component, Component CISOs/ISSMs shall coordinate with the relevant Component SOC and the DHS EOC.	RA-3
5.4.8.f	The DHS EOC shall be notified before any ISVM scans are run.	RA-5
5.4.8.g	System Owners shall report the security alert and advisory status of the information system to the AO, Component CISO/ISSM, and DHS CISO upon request and on a periodic basis.	SI-5

5.4.9 Peer-to-Peer Technology

Policy ID	DHS Policy Statements	Relevant Controls
5.4.9.a	Peer to peer software technology is prohibited on any DHS information system.	CM-7, SA-6

5.5 Cryptography

Cryptography is a branch of mathematics that deals with the transformation of data. Transformation converts ordinary text (plaintext) into coded form (ciphertext) by encryption; and ciphertext into plaintext by decryption.

5.5.1 Encryption

Encryption is the process of changing plaintext into ciphertext for the purpose of security or privacy.

Policy ID	DHS Policy Statements	Relevant Controls
5.5.1.a	Systems requiring encryption shall comply with the following methods: Products using FIPS 197 Advanced Encryption Standard (AES) algorithms with at least 256 bit encryption that has been validated under FIPS 140-2, National Security Agency(NSA) Type 2, or Type 1 encryption. (Note: The use of triple Data Encryption Standard [3DES] and FIPS 140-1 is no longer permitted.)	IA-7, SC-13
5.5.1.b	Components shall develop and maintain encryption plans for sensitive information systems.	IA-7, SC-13
5.5.1.c	Components shall use only cryptographic modules that are FIPS 197 (AES-256) compliant and have received FIPS 140-2 validation at the level appropriate to their use.	IA-7, SC-13

5.5.2 Public Key Infrastructure

A PKI is an architected set of systems and services that provide a foundation for enabling the use of public key cryptography. This is necessary in order to implement strong security services and to allow the use of digital signatures.

The principal components of a PKI are the public key certificates, registration authorities (RA), certification authorities (CA), directory, certificate revocation lists (CRL), and a governing certificate policy (CP.)

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.a	The DHS CISO shall be the DHS PKI Policy Authority (PKI PA) to provide PKI policy oversight. A detailed description of DHS PKI PA roles and responsibilities are provided in the DHS PKI Policy.	SC-17
5.5.2.b	The DHS CISO shall represent DHS on the Federal PKI Policy Authority (FPKI PA.)	SC-17
5.5.2.c	The DHS PKI PA shall appoint a PKI Management Authority (PKI MA) to provide management and operational oversight of the DHS PKI. A detailed description of DHS PKI MA roles and responsibilities are provided in the DHS PKI Policy.	SC-17
5.5.2.d	The DHS PKI shall be governed by the U.S. Common Policy Framework certificate policy approved by the FPKI PA, and the DHS PKI Policy approved by the DHS PKI PA.	SC-17
5.5.2.e	DHS shall have a single DHS Principal CA that is subordinate to the U.S. Common Policy Root CA. The DHS Principal CA shall be operated for DHS by the Department of Treasury (DoT) under the Federal Shared Service Provider (SSP) program.	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.f	All additional CAs within DHS must be subordinate to the DHS Principal CA. The requirements and process for becoming a subordinate CA to the DHS Principal CA shall be specified in the DHS PKI Policy.	SC-17
5.5.2.g	Components that implement a CA shall ensure that the CA is subordinate to the DHS Principal CA.	SC-13
5.5.2.h	All DHS CAs shall have a trust path resolving to the U.S. Common Policy Root CA. The U.S. Common Policy Root CA is cross-certified with the Federal Bridge CA at the high, medium hardware, and medium assurance levels.	SC-17
5.5.2.i	The DHS Principal CA shall operate under an X.509 Certification Practices Statement (CPS). The CPS shall comply with the U.S. Common Policy Framework. DoT, as the SSP for DHS, approves the CPS for the DHS Principal CA.	SC-17
5.5.2.j	All DHS CAs subordinate to the DHS Principal CA shall operate under an X.509 CPS. The CPS shall comply with the U.S. Common Policy Framework and the DHS PKI Policy. The DHS PKI PA must approve the CPS.	SC-17
5.5.2.k	The DHS PKI PA shall ensure that the CPS for each subordinate DHS CA complies with the U.S. Common Policy Framework and DHS PKI Policy prior to approval.	SC-17
5.5.2.l	The DHS PKI MA shall ensure that every subordinate DHS CA operates in compliance with its approved CPS.	SC-17
5.5.2.m	All DHS CAs shall undergo regular PKI compliance audits as required by the U.S. Common Policy Framework and the DHS PKI Policy. The DHS PKI PA shall approve the auditor. The audit findings, report, and POA&Ms to address deficiencies found shall be provided to the DHS PKI PA and DHS PKI MA.	SC-17
5.5.2.n	All DHS CAs shall archive records as required by the U.S. Common Policy Framework and their CPS.	SC-17
5.5.2.o	All operational PKI facilities shall be established in accordance with U.S. Common Policy Framework physical security requirements based on the CA's assurance level and its intended use. Location/protection of the CA shall be determined by its level of assurance. Measures taken to ensure the continuity of PKI operations shall at least provide the same level of availability of PKI Services as the individual and composite availability requirements of the systems and data protected by the certificates.	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.p	The DHS Principal CA and DHS subordinate CAs shall only issue certificates to internal DHS entities, e.g., employees, contractors, roles, groups, applications, code signers, and devices. External entities who require certificates to securely interact with DHS shall acquire certificates from a non-DHS PKI that is cross-certified with the FBCA at medium assurance or above.	SC-17
5.5.2.q	Only the DHS Principal CA shall issue certificates to DHS employees, contractors, roles, code signers, and other human entities, including certificates for DHS HSPD-12 Personal Identify Verification (PIV) Cards. The DHS Principal CA may also issue all other types of certificates allowed under the U.S. Common Policy to internal DHS entities.	SC-17
5.5.2.r	DHS Subordinate CAs shall only issue certificates to internal non-human entities. Any additional restrictions on the types of certificates that may be issued by a specific subordinate DHS CA shall be determined during the subordination process and approved by the DHS PKI PA.	SC-17
5.5.2.s	The use by DHS of any non-DHS service provider for CA or PKI services is prohibited unless approved by the DHS CISO.	SC-13
5.5.2.t	Only certificates that are issued by the DHS Principal CA or a subordinate DHS CA under the U.S. Common Policy Framework at medium assurance or above shall be used to protect sensitive DHS data or to authenticate to operational systems containing sensitive data. Certificates issued by DHS CAs that are not established as subordinate to the DHS Principal CA, certificates issued by test, pilot, third party, self-signed or other CAs shall not be used to protect sensitive data, or to authenticate to DHS operational systems containing sensitive data.	SC-17

5.5.3 Public Key/Private Key

A public key certificate is used to obtain subscribers' public keys in a trusted manner. Once obtained, the public key is then used:

- To encrypt data for that subscriber so that only that subscriber can decrypt it
- To verify that digitally signed data was signed by that subscriber, thereby authenticating the identity of the signing subscriber, and the integrity of the signed data

Policy ID	DHS Policy Statements	Relevant Controls
5.5.3.a	Separate public/private key pairs must be used for encryption and digital signature by human subscribers, organization subscribers, application subscribers, and code-signing subscribers.	SC-12
5.5.3.b	Separate public/private key pairs must be used for encryption and digital signature by device subscribers whenever supported by the protocols native to	SC-12

Policy ID	DHS Policy Statements	Relevant Controls
	the type of device.	
5.5.3.c	A human sponsor shall represent each application, role, code-signing, and device subscriber when it applies for one or more certificates from a DHS CA.	SC-12
5.5.3.d	An authorized DHS employee shall sponsor DHS contractors and other affiliates when they apply for one or more certificates from a DHS CA.	SC-12
5.5.3.e	A mechanism shall be provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, role, application, code signer, or device to receive one or more certificates.	SC-12
5.5.3.f	A mechanism shall be provided for each DHS CA to enable PKI registrars to determine and verify the identity of the authorized human sponsor for each DHS contractor, affiliate, role, application, code signer, or device.	SC-12
5.5.3.g	Human subscribers shall not share private keys and shall be responsible for their security and use. If a human subscriber discloses or shares his or her private key, the subscriber shall be accountable for all transactions signed with the subscriber's private key.	---
5.5.3.h	Sponsors for non-human subscribers (role, application, code-signing, or device) shall be responsible for the security of and use of the subscriber's private keys. Every sponsor shall read, understand, and sign a "DHS PKI Device Sponsor Agreement" as a pre-condition for sponsoring non-human subscribers.	SC-17
5.5.3.i	Subscriber private keys shall not be used by more than one entity, with the following exception. Multiple devices in a high availability configuration may use a single Secure Socket Layer (SSL) Subject Alternative Name (SAN) certificate, and thus use the same key pair.	SC-12
5.5.3.j	Every human subscriber shall read, understand, and sign a "DHS PKI Human Subscriber Agreement" as a pre-condition for receiving certificates from a DHS CA. These signed agreements shall be maintained by the DHS PKI MA.	SC-17

5.6 Malware Protection

Policy ID	DHS Policy Statements	Relevant Controls
5.6.a	Component CISOs/ISSMs shall establish and enforce Component-level malware protection control policies.	SI-3
5.6.b	Components shall implement a defense-in-depth strategy that: - Installs antivirus software on desktops and servers	SI-3

Policy ID	DHS Policy Statements	Relevant Controls
	- Configures antivirus software on desktops and servers to check all files, downloads, and email - Installs updates to antivirus software and signature files on desktops and servers in a timely and expeditious manner without requiring the end user to specifically request the update - Installs security patches to desktops and servers in a timely and expeditious manner	
5.6.c	System Owners shall develop and enforce procedures to ensure proper malware scanning of media prior to installation of primary hard drives, software with associated files, and other purchased products.	AC-20, SI-3

5.7 Product Assurance

Policy ID	DHS Policy Statements	Relevant Controls
5.7.a	Information Assurance (IA) shall be considered a requirement for all systems used to input, process, store, display, or transmit sensitive or national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated COTS IA and IA-enabled IT products. These products shall provide for the availability of systems. The products also shall ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.	---
5.7.b	*Strong preference* shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated, as appropriate, in accordance with the following: - The NIST FIPS validation program - The NSA/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program - The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement	---
5.7.c	The evaluation and validation of COTS IA and IA-enabled products shall be conducted by accredited commercial laboratories or by NIST.	---
5.7.d	Components shall use only cryptographic modules that meet the requirements set forth in Section 5.5, Cryptography.	---
5.7.e	Transaction-based systems (e.g., database management systems, transaction processing systems) shall implement transaction rollback and transaction	---

Policy ID	DHS Policy Statements	Relevant Controls
	journaling, or technical equivalents.	

6.0 DOCUMENT CHANGE REQUESTS

Changes to DHS *Sensitive Systems Policy Directive 4300A* and to the DHS 4300A *Sensitive Systems Handbook* may be requested in accordance with Section 1.7, Changes to Policy.

7.0 QUESTIONS AND COMMENTS

For clarification of DHS information security policies or procedures, contact the DHS Director for Information Systems Security Policy at INFOSEC@dhs.gov.

APPENDIX A ACRONYMS

AC	Access Control
AES	Advanced Encryption Standards
AO	Authorizing Official
ARB	Acquisition Review Board
AT	Awareness and Training
ATO	Authority to Operate
AU	Audit and Accountability
BI	Background Investigation
BIA	Business Impact Assessment
BLSR	Baseline Security Requirements
CA	Certificate Authority Certification, Accreditation, and Security Assessments
CCB	Change Control Board
CFO	Chief Financial Officer
CI	Counter-Intelligence
C-I-A	Confidentiality, Integrity, and Availability
CIO	Chief Information Officer
CISID	Chief, Internal Security and Investigations Division
CISO	Chief Information Security Officer
CM	Configuration Management
CMG	Core Management Group
CMP	Configuration Management Plan
CO	Certifying Official
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan Continuity of Operations Planning
COTS	Commercial off the Shelf
CP	Contingency Plan Contingency Planning Certificate Policy

CPIC	Capital Planning and Investment Control
CPS	Certificate Practices Statement
CRE	Computer-Readable Extract
CRL	Certificate Revocation List
CSIRC	Computer Security Incident Response Center
CSO	Chief Security Officer
CUI	Control Unclassified Information
DES	Digital Encryption Standards
DHS	Department of Homeland Security
DNSSEC	Domain Name System Security Extensions
DoD	Department of Defense
DoS	Department of State
DoT	Department of Treasury
EA	Enterprise Architecture
EAB	Enterprise Architecture Board
EO	Executive Order
EOC	Enterprise Operations Center
FBCA	Federal Bridge Certification Authority
FDCC	Federal Desktop Core Configuration
FICAM	Federal Identity, Credentialing, and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOUO	For Official Use Only
FPKI PA	Federal PKI Policy Authority
FTP	File Transfer Protocol
FYHSP	Future Years Homeland Security Program
GSA	General Services Administration
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
HSAR	Homeland Security Acquisition Regulations

HSDN	Homeland Secure Data Network
HSPD	Homeland Security Presidential Directive
HVAC	Heating, Ventilation and Air Conditioning
IA	Identification and Authentication Information Assurance
IATO	Interim Authority to Operate
ICAM	Identity, Credentialing, and Access Management
IDS	Intrusion Detection System
IR	Incident Response Infrared
IRB	Investment Review Board
ISA	Interconnection Security Agreement
ISO	Information Security Office
ISSO	Information System Security Officer
ISVM	Information System Vulnerability Management
JWICS	Joint Worldwide Intelligence Communications System
IT	Information Technology
LAN	Local Area Network
LE	Law Enforcement
LMR	Land Mobile Radio
MA	Maintenance Major Application
MBI	Minimum Background Investigation
MD	Management Directive
MMS	Multimedia Messaging Service
MP	Media Protection
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NSA	National Security Agency
OCIO	Office of the Chief Information Officer

OID	Object identifier
OIG	Office of Inspector General
OIS	Office of Information Security
OMB	Office of Management and Budget
OPA	Office of Public Affairs
OPM	Office of Personnel Management
OTAR	Over-The-Air-Rekeying
PA	Policy Authority
PBX	Private Branch Exchange
PCS	Personal Communications Services
PDA	Personal Digital Assistant
PE	Physical and Environmental Protection
PED	Portable Electronic Device
PEP	Policy Enforcement Point
PHI	Protected Health Information
PIRT	Privacy Incident Response Team
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identity Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
PKI PA	PKI Policy Authority
PKI PM	PKI Management Authority
PL	Planning
PM	Program Manager Program Management
PNS	Protected Network Services
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPOC	Privacy Point of Contact
PS	Personnel Security

PSTN	Public Switched Telephone Network
PTA	Privacy Threshold Analysis
RA	Risk Assessment Registration Authority
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFID	Radio Frequency Identification
RMS	Risk Management System
SA	Security Architecture System and Services Acquisition
SAN	Subject Alternative Name
SAR	Security Assessment Report
SAISO	Senior Agency Information Security Officer
SAOP	Senior Agency Official for Privacy
SC	System and Communications Protection
SCI	Sensitive Compartmented Information
SELC	Systems Engineering Life Cycle
SI	System and Information Integrity
SLA	Service Level Agreement
SMS	Short Message Service
SOC	Security Operations Center
SOP	Standard Operating Procedure
SORN	System of Records Notice
SP	Special Publication Security Plan
SSH	Secure Shell
SSL	Secure Socket Layer
SSP	Shared Service Provider
TAF	TrustedAgent FISMA
TFPAP	Trust Framework Provider Adoption Process
TIC	Trusted Internet Connections

TOS	Terms of Service
TRM	Technical Reference Model
TS	Top Secret
US-CERT	United States Computer Emergency Readiness Team
VA	Vulnerability Assessment
VAT	Vulnerability Assessment Team
USGBC	U.S. Government Configuration Baseline
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

APPENDIX B GLOSSARY

The following definitions apply to the policies and procedures outlined in this document. Other definitions may be found in NIST IR 7298, *Glossary of Key Information Security Terms* and the National Information Assurance (IA) Glossary.

Acceptable Risk	Mission, organizational, or program-level risk deemed tolerable by the RE after adequate security has been provided.
Accreditation Package	The documents submitted to the AO for the Accreditation Decision. An Accreditation Package consists of: Accreditation Decision Letter Security Plan - criteria provided on when the plan should be updated Security Assessment Report - updated on an ongoing basis whenever changes are made to either the security controls in the information system or the common controls inherited by those systems Plan of Action and Milestones
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. [OMB Circular A-130, Appendix III]
Annual Assessment	DHS activity for meeting the annual FISMA self-assessment requirement.
Authorizing Official (AO)	An official within a Federal Government agency who can grant approval for a system to operate.
Cellular phone	A mobile device used for voice communication irrespective of the communications technology employed.
Certification/ Certifying Agent	A contractor that performs certification tasks as designated by the CO.
Certifying Authority (CA)	Obsolete term; see Security Control Assessor
Security Control Assessor	A senior management official who certifies the results of the security assessment. He or she must be a Federal Government employee.
Chief Information Officer (CIO)	The executive within a Federal Government agency responsible for its information systems.

Compensating Control	An internal control intended to reduce the risk of an existing or potential control weakness.
Component	A DHS Component is any of the entities within DHS, including all DHS offices and independent agencies.
Computer Security Incident Response Center	DHS organization that responds to computer security incidents.
Designated Approval Authority (DAA)	Obsolete term; see Authorizing Official (AO).
Information System	Any information technology that is (1) owned, leased, or operated by any DHS Component, (2) operated by a contractor on behalf of DHS, or (3) operated by another Federal, state, or local Government agency on behalf of DHS. Information systems include general support systems and major applications.
Enterprise Operations Center (EOC)	The DHS organization that coordinates security operations for the DHS Enterprise.
Exception	Acceptance to permanently operate a system that does not comply with policy.
For Official Use Only	The marking instruction or caveat "For Official Use Only" will be used to identify sensitive but unclassifed information within the DHS community that is not otherwise specifically described and governed by statute or regulation.
General Support System (GSS)	An interconnected set of information resources under the same direct management control and sharing common functionality. A GSS normally includes hardware, software, information, applications, communications, data, and users.
Information Security Vulnerability Management (ISVM)	DHS system that provides notification of newly discovered vulnerabilities and tracks the status of vulnerability resolution.
Information System Security Officer (ISSO)	Someone who implements and/or monitors security for a particular system.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Major Application (MA)	An automated information system (AIS) that "requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application" in accordance with OMB Circular A-130. An MA is a discrete application, whereas a GSS may support multiple applications.
Management Controls	The security controls for an information system that focus on the management of risk and the management of information system security.
Operational Controls	The security controls for an information system that are primarily implemented and executed by people (as opposed to systems).
Operational Risk	The risk contained in a system under operational status. It is the risk that an AO accepts when granting an ATO.
Personally Identifiable Information (PII)	Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to an individual regardless of whether the individual is a U.S. Citizen, legal permanent resident, or a visitor to the U.S.
Pilot	A test system in the production environment that may contain operational data and may be used to support DHS operations, typically in a limited way.
Policy Statement	A high-level rule for guiding actions intended to achieve security objectives.
Policy Enforcement Point (PEP)	A firewall or similar device that can be used to restrict information flow.
Portable Electronic Device (PED)	A device that has a battery and is meant to process information without being plugged into an electric socket; it is often handheld but can be a laptop computer.
Privacy Sensitive System	Any system that collects, uses, disseminates, or maintains PII or sensitive PII.
Production	Operational, as in "production system" or "production environment."
Prototype	A test system in a test environment that must not contain operational data and must not be used to support DHS operations.
Remote Access	Access to a DHS information system by a user (or an information system) communicating through an external, non-DHS-controlled network (e.g., the Internet).
Residual Risk	The risk remaining after security controls have been applied.

Risk Executive (RE)	An individual who ensures that risks are managed consistently across the organization. An RE can be at the Departmental or Component level.
Security Control	A particular safeguard or countermeasure to protect the confidentiality, integrity, and availability of a system and its information.
Security Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Security Operations Center (SOC)	The DHS Component organization that coordinates security operations within its Component.
Security Requirement	A formal statement of action or process applied to an information system and its environment in order to provide protection and attain security objectives. Security requirements for any given system are contained in its Security Plan.
Senior Agency Information Security Official (SAISO)	The point of contact within a Federal Government agency responsible for its information system security.
Sensitive But Unclassified	Obsolete designation; see Sensitive Information.
Sensitive Information	Information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal Government programs or other programs or operations essential to the national interest.
Sensitive Personally Identifiable Information (Sensitive PII)	PII that requires stricter handling guidelines because of the nature of the data and the increased risk to an individual if compromised, and if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of sensitive PII include Social Security numbers or alien number (A-number).
Significant Incident	A computer security-related incident that represents a meaningful threat to the DHS mission and requires immediate leadership notification.
Spam	E-mails containing unwanted commercial solicitation, fraudulent schemes, and possibly malicious logic.
Strong Authentication	Layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information.
System	A discrete set of information system assets contained within the accreditation boundary.

System Owner	??
Technical Controls	The security controls for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware elements of the system.
Two-Factor Authentication	Authentication can involve something the user knows (e.g., a password), something the user has (e.g., a smart card), or something the user "is" (e.g., a fingerprint or voice pattern). Single-factor authentication uses only one of the three forms of authentication, while two-factor authentication uses any two of the three forms. Three-factor authentication uses all three forms.
Unclassified Information	Information that has not been determined to be classified pursuant to Executive Order 13526, as amended
USB Device	A device that can be connected to a computer by its USB plug.
USB Drive	A memory device small enough to fit into a pocket and that connects to a computer by its USB plug.
Vulnerability Scanning	An automated scan for potential security vulnerabilities.
Waiver	Acceptance to temporarily operate a system that does not comply with policy while working towards compliance.

APPENDIX C REFERENCES

The DHS information security program and organization are based upon public laws, executive orders, national policy, external guidance, and internal DHS guidance.

Public Laws and U.S. Code

- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, DC, July 14, 1987
- Public Law 107-347, *E-Government Act* of 2002, including Title III, *Federal Information Security Management Act (FISMA)*
- Public Law 104-106, *Clinger-Cohen Act* of 1996 [formerly, Information Technology Management Reform Act (ITMRA)]
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*
- Public Law 100-235, *Computer Security Act* of 1987 as amended
- Public Law 93-579, *Freedom of Information Act* of 2002 as amended

Executive Orders

- Executive Order 13526, *Classified National Security Information*, December 29, 2009
- Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004

Office of Management and Budget Directives

- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*
- OMB Bulletin 06-03, *Audit Requirements for Federal Financial Statements*
- OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies,* December 16, 2003
- OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006
- OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007
- OMB Memorandum M-09-02, *Information Technology Management Structure and Governance Framework, October 21, 2008*
- OMB Memorandum 10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, April 21, 2010

- OMB Memorandum 10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS),* July 6, 2010
- OMB Memorandum 11-06, *WikiLeaks - Mishandling of Classified Information*, November 28, 2010

Other External Guidance

- Intelligence Community Directive Number 508, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*, September 15, 2008
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS), including:
    - NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
    - NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
- NIST Information Technology Security Special Publications (SP) 800 series, including:
    - NIST SP 800-16, Rev 1, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (Draft)
    - NIST SP 800-34, Rev 1, *Contingency Planning Guide for Information Technology Systems*
    - NIST SP 800-37, Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
    - NIST SP 800-39, *Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View* (Draft)
    - NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
    - NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*
    - NIST SP 800-53, Rev 3*, Recommended Security Controls for Federal Information Systems and Organizations*
    - NIST SP 800-53A, Rev 1, *Guide for Assessing the Security Controls in Federal Information Systems*
    - NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*
    - NIST SP 800-63, Rev 1, *Electronic Authentication Guideline* (Draft)
    - NIST SP 800- 65, Rev 1, *Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process (CPIC) (Draft)*

- NIST SP 800-88, *Guidelines for Media Sanitization*
- NIST SP 800-92, *Guide to Computer Security Log Management*
- NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*
- NIST SP 800-95, *Guide to Secure Web Services*
- NIST SP 800-100, *Information Security Handbook: A Guide for Manager*
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*
- NIST SP 800-118, *Guide to Enterprise Password Management* (Draft)
- *NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- NIST SP 800-123, *Guide to General Server Security*
- NIST SP 800-124, *Guidelines on Cell Phone and PDA Security*
- NIST SP 800-128, *Guide for Security Configuration Management of Information Systems* (Draft)
- NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (Draft)

- NIST IR 7298, *Glossary of Key Information Security Terms*
- CNSS Instruction No. 4009, *National Information Assurance Glossary*
- CNSS Instruction No. 1001, *National Instruction on Classified Information Spillage*

Internal Guidance

- Department of Homeland Security Acquisition Regulation (HSAR)
- DHS Management Directives (MD), especially:
  - MD 140-01, *Information Technology Systems Security*
  - MD 11042.1, *Safeguarding Sensitive but Unclassified (For Official Use Only) Information*
  - MD 102-01 *Acquisition Management*
  - MD 1030, *Corrective Action Plans*
  - MD 4400.1, *DHS Web and Information Systems*
  - MD 4500.1, *DHS Email Usage*
  - MD 4600.1, *Personal Use of Government Office Equipment*
  - MD 4900, *Individual Use and Operation of DHS Information Systems/Computers*
  - MD 11055, *Suitability Screening Requirements for Contractor Employees*

APPENDIX D DOCUMENT CHANGE HISTORY

Version	Date	Description
0.1	December 13, 2002	Draft Baseline Release
0.2	December 30, 2002	Revised Draft
0.5	January 27, 2003	Day One Interim Policy
1.0	June 1, 2003	Department Policy
1.1	December 3, 2003	Updated Department Policy
2.0	March 31, 2004	Content Update
2.1	July 26, 2004	Content Update
2.2	February 28, 2005	Content Update
2.3	March 7, 2005	Content Update
3.0	March 31, 2005	Includes updates to PKI, Wireless Communications, and Media Sanitization (now Media Reuse and Disposition) sections
3.1	July 29, 2005	New policies: 3.1b,e,f, 3.1g. 4.1.5b, 4.8.4a. Modified policies: 3.7b, c, 3.9b,g, 3.10a, 4.3.1b, 4.8.2a, 4.8.5e, 5.1.1b, 5.2.2a, 5.3a, c, 5.4.1a, 5.4.5d, 5.4.8c, 5.5.1a, 5.7d. Policies relating to media disposal incorporated into policies within Media Reuse and Disposition section. Deleted policy regarding use of automated DHS tool for conducting vulnerability assessments.
3.2	October 1, 2005	Modified policies 3.8b, 4.8.1a, 5.2.1a&b, 5.2.2a, and 5.4.3c; combined (with modifications) policies 4.1e and 4.1f; modified Section 1.5
3.3	December 30, 2005	New policies: policies 3.9a–d; 3.11.1b; 4.3.1a; 4.6c; 5.4.3d&e. Modified policies: policies 3.9i&j; 4.3.2a; 4.6a, b; 4.6.1e; 4.6.2j; 4.6.2.1a; 4.6.3e; 5.4.3c; 5.5.2k. Modified sections: 2.5, 2.7, 2.9, 2.11, 3.9, 5.5.2.
4.0	June 1, 2006	New policies: 3.5.3.c&g, 4.6.2.3.c, 5.1.c, 5.2.c, 5.4.1.a. Modified policies: 3.5.1.c, 3.5.3.d–f, 3.7.a&b, 3.9.a&b, d, 4.1.4.b&c, 4.2.1.a, 4.3.1.a, 4.6.c, 4.6.1.a, 4.6.2.f, 4.10.3.a, 5.2.1.b, 5.3.a&b, 5.4.1.b, 5.4.3.c, 5.4.5.d. Modified section: Section 2.9.
4.1	September 8, 2006	New policies: 3.14.1.a–c; 3.14.3.a–c; 4.10.1.c; 5.3.d&e; 5.4.1.c–e. Modified policies: 3.9.b; 4.6.2.d; 4.8.2.a–c; 4.10.1.b; 5.1.c; 5.3.c; 5.4.1.b. New sections: 3.14, 3.14.1, 3.14.3. Modified sections: 2.9, 4.8.2.
4.2	September 29, 2006	New policies: 4.6.4.a–f. Modified policies: 4.3.3.a–c. New section: 4.6.4.
5.0	March 1, 2007	New policies: 4.1.5.h. Modified policies: 3.10.c, 4.1.1.d, 4.1.5.a,b,f, &g, 4.6.2.d, 4.6.3.f, 5.2.c, 5.4.8.a, 5.6.b. New sections: 4.1.1. Modified

Version	Date	Description
		sections: 1.2, 1.4.2, 1.4.3, 2.9, 3.12, 4.1 and subsections, 4.6.1–4.6.4, 4.9, 5.2.1. Renumbered sections: 4.1.2–4.1.6, 4.9, 4.10, 4.11, 4.12.
5.1	April 18, 2007	Update based on SOC CONOPS, Final Version 1.4.1, April 6, 2007; Adds DHS Chief Financial Officer – Designated Financial Systems; Updates the term, *Sensitive But Unclassified* to *For Official Use Only*
5.2	June 1, 2007	Updates Sections 2.7, 2.9, 2.12, 3.3, 3.5.1, 3.5.3, 3.6, 3.8, 3.9, 3.10, 3.14, 3.15, 4.1.5, 4.1.6, 4.10, 4.12, 5.1.1, 5.2, 5.3, 5.4.1, 5.4.3, 5.4.4, 5.4.8, 5.5.1, 5.7
5.3	August 3, 2007	Revised policy in Sections 3.5.1 and 5.5.1, and removed Section 3.5.2. Removed Sections 3.11.2 and 3.11.4
5.4	October 1, 2007	Content update, incorporation of change requests
5.5	September 30, 2007	**Section 1.0:** 1.1 – Added text regarding policy implementation and DHS security compliance tool updates. 1.2 – Removed two references from list; deleted "various" from citation of standards. **Section 2.0:** 2.0 – Insert the following after the first sentence in the second paragraph: “Security is an inherently governmental responsibility. Contractors and other sources may assist in the performance of security functions, but a government individual must always be designated as the responsible agent for all security requirements and functions.” 2.3 – Removed parentheses from "in writing." **Section 3.0:** 3.9 – Inserted new policy element “l” regarding CISO concurrence for accreditation. 3.15 – Added text regarding Component CFOs and ISSMs. **Section 4.0:** 4.1.1 – Capitalized “Background,” and added "(BI)." 4.3.1 – Two new elements were added to the policy table. 4.7 – Inserted "where required or appropriate" before the sentence. 4.8.3 – Title changed to “Personally Owned Equipment and Software (not owned by or contracted for by the Government).” 4.8.6 – Included new section regarding wireless settings for peripheral equipment. **Section 5.0:** 5.1c – Changed inactive accounts to “disable user identifiers after forty-five (45) days of inactivity.” 5.1.1 – First sentence of the second paragraph was rewritten to prohibit use of personal passwords by multiple individuals. 5.2.2 – Title changed to “Automatic Session Termination.”
6.0	May 14, 2008	**Global change** “Shoulds” changed to “shalls” throughout the document. Replaced certain instances of “will” with “shall” throughout document to indicate compliance is required. Various changes were made throughout the document to ensure that the 4300A Policy and Handbook align with the 4300B Policy and Handbook. “ISSM” changed to “CISO/ISSM” throughout the document. "CPO" changed to "Chief Privacy Officer" throughout the document. “IT Security Program” changed to “Information Security Program”

Version	Date	Description
		throughout the document." "System Development Life Cycle" changed to "System Life Cycle" and "SDLC" changed to "SLC" throughout the document. **Title Page** Title page of 4300A Policy - Language on the Title Page was reworded. "This is the implementation of DHS Management Directive 4300.1." **Section 1.0** 1.1 – Updated to clarify 90 day period in which to implement new policy elements. 1.2 – Added OMB, NIST, and CNSS references. 1.4 – Added reference and link to Privacy Incident Handling Guidance and the Privacy Compliance documentation. 1.4.2 – Added definition of National Intelligence Information. 1.4.3 – Inserted definition of National Security Information to align with 4300B Policy. 1.4.8.1 – Definition of General Support System was updated. 1.4.8.2 – Definition of Major Application was updated. 1.4.10 – Section was renamed "Trust Zone." 1.4.16 – Inserted new definition for FISMA. 1.5 – Language was updated to increase clarity for financial system owners for waivers and exceptions. **Section 2.0** 2.3 – Added a new responsibility for DHS CIO. 2.4 – Added a new responsibility for Component CIOs. 2.5 - Chief Information Security Officer (CISO) renamed DHS Chief Information Security Officer (CISO). Updated to include privacy-related responsibilities. 2.6 – Added a new section in Roles and Responsibilities called "Component CISO." 2.7 – Updated Component ISSM Role and Responsibilities. 2.8 – Changed name of the section from "Office of the Chief Privacy Officer (CPO)" to "The Chief Privacy Officer". Updated to include privacy-related responsibilities. 2.9 – Added a new role for DHS CSO. 2.10 – Updated to include privacy-related responsibilities. 2.11 - Added privacy-related responsibilities. 2.12 – Added a new section, "OneNet Steward." 2.13 – Added a new section, "DHS Security Operations Center (DHS SOC) and Computer Security Incident Response Center (CSIRC)."

Version	Date	Description
		2.14 – Added a new section, "Homeland Secure Data Network (HSDN) Security Operations Center (SOC)." 2.16 – Added a new section, "Component-level SOC." 2.18 – Updated to include privacy-related responsibilities. 2.19 – Last sentence of first paragraph has been updated to say: "ISSO Duties shall not be assigned as a collateral duty. Any collateral duties shall not interfere with their ISSO duties." 2.20 – Updated to include privacy-related responsibilities. **Section 3.0** 3.9 – Added C&A information for unclassified, collateral classified and SCI systems. Also, prior to DHS Policy table, included sentence regarding C&A. 3.9.b – Language updated to clarify that a minimum impact level of moderate is required for confidentiality for CFO designated financial systems. 3.9.h – New guidance is provided to clarify short term ATO authority. 3.11.1 – Added new section discussing the CISO Board. 3.11.3 – Removed DHS Wireless Security Working Group. 3.14.1 – Added new text defining PII and sensitive PII. At the end of bullet #4, added definition of computer-readable data extracts. Updated 3.14.1.a and 3.14.1.b based on input from the Privacy Office. Added sentence "DHS has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. 3.14.2 - Added new section called "Privacy Threshold Analyses." 3.14.3 - Updated Privacy Impact Assessment Responsibilities table. 3.14.4 - Added new section called "System of Record Notices." **Section 4.0** 4.1.5.c – Updated to address training requirements. 4.1.5.g – Deleted "Training plans shall include awareness of internal threats and basic IT security practices." 4.1.5.h (now 4.1.5.g) – Updated to include the following sentence: "Components shall account for Contingency Plan Training, and Incident Response Training conducted for Moderate and High IT Systems." 4.3.1.d – FIPS 140-2 compliance language was updated. 4.8.1.a and 4.8.1.c – Language has been updated to provide clarification of timeout values. 4.8.2.a – FIPS 140-2 compliance language was updated. 4.8.2.b – Added a new policy element regarding powering down laptops when not in use. 4.9 – Section was renamed "Department Information Security Operations." 4.9, 4.9.1, 4.9.2 – Updated policy elements to support Department security

Version	Date	Description
		operations capabilities, based on the SOC CONOPS. 4.9.2.b – Updated to say "Components shall obtain guidance from the DHS SOC before contacting local law enforcement except where there is risk to life, limb, or destruction of property." 4.12.a – Added policy element to align with Handbook. **Section 5.0** 5.2.1.a, 5.2.1.b, and 5.2.1.c – Language has been updated to provide clarification of timeout values. 5.2.2 Introductory language, 5.2.2.a, 5.2.2.b, and 5.2.2.c – Language and policy updated to clarify the meaning of a session termination. 5.3.f - Updated to clarify responsibilities of the System Owner regarding computer-readable data extracts. 5.4.1.d – Added sentence "DHS has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access." 5.4.3.a through i – New guidance is provided regarding the preparation of ISAs for interconnections to the DHS OneNetwork. 5.4.3.g – Replaced "interconnect service agreements" with "interconnection security agreements." 5.4.4.f - New guidance is provided regarding internal firewalls. 5.4.5.f – New guidance is provided regarding the use of the RDP protocol. 5.4.6 – Added text "NOTE: Due to many attacks that are HTML-based, please note that DHS will be following the lead of the DoD and moving to text based email." 5.4.8.a – Language updated to reflect that annual vulnerability assessments should be conducted. 5.4.8.f – Policy updated to clarify automated system scanning. 5.5.1.c – Updated element to specify usage of cryptographic modules that "are FIPS 197 compliant and have received FIPS 140-2 validation." 5.5.2.f – Policy updated to clarify hosting of DHS Root CA.
6.1	September 23, 2008	**Global Changes** Replaced all instances of "CISO/ISSM" with "Component CISO/ISSM." Replaced all DHS-related instances of "agency/agency-wide" with "Department/Department-wide." Replaced all instances of "24x7" with "continuous" or "continuously," as appropriate. Replaced all instances of "IT security" with "information security." Various minor editorial and grammatical changes were made throughout the document. **Section 1.0** 1.2 – Added reference to E-Government Act of 2002, January 7, 2003.

Version	Date	Description
		1.4 – Replaced "National InfoSec Glossary" with "National Information Assurance (IA) Glossary." 1.4.5 – Replaced third sentence with "System vulnerability information about a financial system shall be considered Sensitive Financial Information." 1.5.2 – Added text regarding acceptance of resulting risk by the Component CFO for financial systems. 1.5.3 – Corrected the title and location of Attachment B. Added text regarding PTA requirements. **Section 2.0** 2.1 – Updated to clarify Secretary of Homeland Security responsibilities. 2.2 – Updated to clarify Undersecretaries and Heads of DHS Components responsibilities. 2.3 – Updated to clarify DHS CIO responsibilities. 2.4 – Updated to clarify Component CIO responsibilities. 2.5 – Updated to clarify DHS CISO responsibilities. 2.6 – Updated to clarify Component CISO responsibilities. 2.8 – Moved "The Chief Privacy Officer" section to 2.9. 2.11 – Updated to clarify Program Managers' responsibilities. 2.14 – Updated to clarify HSDN SOC responsibilities. Updated HSDN SOC unclassified email address. 2.19 – Updated to clarify ISSO responsibilities and the assignment of ISSO duties as a collateral duty. 2.20 – Updated to clarify System Owners' responsibilities. 2.23.2 – Updated to clarify DHS CIO responsibilities for financial systems. **Section 3.0** 3.1.e – Replaced "FISMA and OMB requirements" with "FISMA, OMB, and other Federal requirements." 3.1.h – Replaced "maintain a waiver" with "maintain a waiver or exception." 3.14.1 – Included text regarding the type of encryption needed for laptops. 3.14.3 – Included text stating that the PTA determines whether a PIA is conducted. 3.14.4 – Moved first sentence of second paragraph to be the first sentence of the first paragraph. Included "that are a system of record" after "IT Systems" in the second sentence of the first paragraph. **Section 4.0** 4.3.1.a – Included "locked tape device" in media protection. 4.3.1.d – Updated to clarify that AES 256-bit encryption is mandatory. 4.8.2.a – Updated to clarify that AES 256-bit encryption is mandatory.

Version	Date	Description
		4.8.3.c – Included new policy element regarding use of seized IT equipment. 4.8.4.f – Included new policy element regarding management and maintenance of system libraries. 4.8.5.b – Policy updated to clarify limited personal use of DHS email and Internet resources. 4.9 – First paragraph updated to clarify DHS SOC and HSDN SOC responsibilities. 4.9.b – Updated to specify that the HSDN SOC is subordinate to the DHS SOC. 4.9.1 – First two paragraphs updated to clarify relationship between the DHS SOC and the HSDN SOC. 4.9.1.a – Removed the words "Component SOC." 4.9.1.b – Updated to clarify means of communication for reporting significant incidents. 4.9.1.c – Updated to clarify the length of time by which significant HSDN incidents must be reported. 4.9.1.d. – Updated to clarify reporting for HSDN incidents. **Section 5.0** 5.2.d – Replaced "Component CISO/ISSM" with "Component CISO/ISSM or his/her designee." 5.2.1 – Changed "48 hour time period" to "24 hour time period." 5.4.5.g – Included new policy element regarding blocking of specific Internet websites or categories. 5.4.7 – Updated the policy element to prohibit use of webmail and other personal email accounts. 5.5.1.c – Updated to clarify that AES 256-bit encryption is mandatory. 5.7.d – Included new policy element regarding use of cryptographic modules in order to align with 4300A Handbook. 5.7.e – Included new policy element regarding rollback and journaling for transaction-based systems.
6.1.1	October 31, 2008	5.2.3 – Included new language and a link to the DHS computer login warning banner text on DHS Online.
7.0	July 31, 2009	**General Updates** Added section and reference numbers to policy elements Added NIST 800-53 reference controls to policy elements Added hyperlinks to most DHS references Introduced new terminology Senior Agency Information Security Officer, Risk Executive, and Authorizing Official (AO) – replaces DAA, as per NIST 800-37 and 800-53 Added Appendix A – Acronyms

Version	Date	Description
		Added Appendix B – Glossary Added Appendix C – References list has been updated and moved to Appendix C. (these are detailed references, an abbreviated list is still found at the beginning of the document) Added Appendix D – Change History (This was moved from the front of the document) **Specific Updates** **Section 1.1 – Information Security Program Policy** – Added the statement, "Policy elements are designed to be broad in scope. Specific implementation information can often be found in specific National Institute for Standards and Technology (NIST) publications, such as NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Systems." **Section 1.4.17-19 – Privacy** – Added definitions for PII, SPII, and Privacy Sensitive Systems **Section 1.5 – Exceptions and Waivers** – Updated this section, clarified policy elements, and consolidated all exceptions and waivers requirements. **Section 1.5.4 – U.S. Citizen Exception Requests** – Updated section to include policy elements: 1.5.4.a – Persons of dual citizenship, where one of the citizenships includes U.S. Citizenship, shall be treated as U.S. Citizens for the purposes of this directive. 1.5.4.b – Additional compensating controls shall be maintained for foreign nationals, based on nations lists maintained by the DHS CSO. **Section 1.6 – Information Sharing and Communication Strategy** – Added policy element: 1.6.a - For DHS purposes, electronic signatures are preferred to pen and ink or facsimile signatures in all cases except where pen & ink signatures are required by public law, Executive Order, or other agency requirements. **Section 1.7 – Changes to Policy** – Updated entire section **Section 2.0 – Roles and Responsibilities** – Reformats entire section. Places emphasis on DHS CISO and Component-level Information Security Roles. Secretary and senior management roles are moved to the end of the section. Some specific areas to note include: **Section 2.1.1 – DHS Senior Agency Information Security Officer** – Introduces this term and assigns duties to DHS CISO **Section 2.1.2 – Chief Information Security Officer** – Adds the following responsibilities: - Appoint a DHS employee to serve as the Headquarters CISO - Appoint a DHS employee to serve as the National Security Systems (NSS) CISO **Section 2.1.3 – Component Chief Information Security Officer** – Adds policy element:

Version	Date	Description
		2.1.3.b - All Components shall be responsible to the appropriate CISO. Components without a fulltime CISO shall be responsible to the HQ CISO. Adds 4 additional CISOs to the list of Component CISOs: Federal Law Enforcement Training Center Office of the Inspector General Headquarters, Department of Homeland Security The DHS CISO shall also appoint an NSS CISO **Section 2.1.4 – Component Information Systems Security Manager** – Component CISO now works directly with the HQ CISO, rather than with the DHS CISO. **Section 2.1.5 – Risk Executive** – Introduces this term as per NIST. Assigns responsibilities to CISOs (already performing these functions) **Section 2.1.6 – Authorizing Official** – Introduces this term as per NIST. Replaces the term Designated Approval Authority (DAA) **Section 2.2.10 – DHS Employees, Contractors, and Vendors** – Adds the requirement for vendors to follow DHS Information Security Policy **Section 3.2 – Capital Planning and Investment Control** – Adds policy element: 3.2.f – Procurement authorities throughout DHS shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced. **Section 3.3 – Contractors and Outsourced Operations** – Adds policy element: 3.3.g – Procurement authorities throughout DHS shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced. **Section 3.5.2 – Contingency Planning** – Updates and expands entire section. **Section 3.7 – Configuration Management** – Adds policy elements Section 3.7.f – If the information system uses operating systems or applications that do not have hardening or do not follow configuration guidance from the DHS CISO, the System Owner shall request an exception, including a proposed alternative secure configuration. Section 3.7.g – Components shall ensure that CM processes under their purview include and consider the results of a security impact analysis when considering proposed changes. **Section 3.9 – Certification, Accreditation, and Security Assessments** – Updates entire section **Section 3.11.1 – CISO Council** – Updates the term from CISO Board **Section 3.14-3.14.6 – Privacy Sections** – Updates all sections pertaining to privacy and privacy information, adds section 3.14.5 – Protecting Privacy Sensitive Systems **Section 3.14.7 – E-Authentication** – Renumbers this section from 3.14.6 (due to adding of privacy section 3.14.5

Version	Date	Description
		Section 3.15 – DHS Chief Financial Officer Designated Systems – Section renamed from DHS Chief Financial Officer Designated Financial Systems **Section 3.16 – Social Media** – Added Social Media section to provide guidelines and address the Federal Government's (including DHS) use of social media sites (You Tube, Twitter) **Section 4.1.2 – Rules of Behavior** – Added policy element: 4.1.2.b – Components shall ensure that DHS users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems or data. **Section 4.1.5 – IT Security Awareness, Training, and Education** – Updates entire section **Section 4.1.6 – Separation from Duty** – Updates policy element to require that all assets and data are recovered from departing individuals 4.1.6.b – Components shall establish procedures to ensure that all DHS information system-related property and assets are recovered from the departing individual and that sensitive information stored on any media is transferred to an authorized individual. Adds policy elements: 4.1.6.c - Accounts for personnel on extended absences shall be temporarily suspended. 4.1.6.d – System Owners shall review information system accounts supporting their programs at least annually. **Section 4.3.2 – Media Marking and Transport** – Adds "Transport" to section title and adds policy element: 4.3.2.b – Components shall control the transport of information system media containing sensitive data, outside of controlled areas and restrict the pickup, receipt, transfer, and delivery to authorized personnel. **Section 4.6 – Wireless Network Communications** – Updated section title from "Wireless Communication" and specifies "network communication" technologies in policy, rather than the more general "Wireless." Removes references to the defunct "WMO." **Section 4.6.1 – Wireless Systems** – Adds policy elements: 4.6.1.f – Component CISOs shall review all system applications for wireless usage, maintain an inventory of systems, and provide that inventory to the DHS CISO at least annually. 4.6.1.g – Component CISOs shall (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, and control wireless access to DHS information systems. **4.9.1 – Security Incidents and Incident Response and Reporting** – Adds requirement for Components to maintain full SOC and CSIRC capability (May outsource to DHS SOC). Adds policy elements: 4.9.1.k – Components shall maintain a full SOC and CSIRC capability or outsource this capability to the DHS SOC. The DHS SOC shall provide

Version	Date	Description
		SOC and CSIRC services to Components in accordance with formal agreements. Information regarding incident response capability is available in Attachment F of the DHS 4300A Sensitive Systems Handbook. 4.9.1.q – The DHS CISO shall publish Incident Response Testing and Exercise scenarios as required. 4.9.1.r – The Component CISO for each Component providing an incident response capability shall ensure Incident Response Testing and Exercises are conducted annually in coordination with the DHS CISO. **Section 5.1 – Identification and Authentication** – Adds requirement for strong authentication following HSPD-12 implementation. 5.1.f – Components shall implement strong authentication on servers, for system administrators and significant security personnel, within six (6) months of the Component's implementation of HSPD-12. **Section 5.4.1 – Remote Access and Dial-In** – Updates section and adds policy element: 5.4.1.f – The Public Switched Telephone Network (PSTN) shall not be connected to OneNet at any time. **5.4.3 – Network Connectivity** – Requires DHS CIO approval for all network connections outside of DHS. Also specifies requirement for CCB. 5.4.3.g – The DHS CIO shall approve all interconnections between DHS information systems and non-DHS information systems. Components shall document interconnections with an ISA for each connection. The DHS CIO shall ensure that connections with other Federal Government Agencies are properly documented. A single ISA may be used for multiple connections provided that the security accreditation is the same for all connections covered by that ISA. 5.4.3.l - The appropriate CCB shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline. DHS systems that interface with OneNet shall also be subject to the OneNet CCB. **Section 5.4.4 – Firewalls and Policy Enforcement Points** – Updates language to include Policy Enforcement Points. Adds policy elements: 5.4.4.i – The DHS CISO shall establish policy to block or allow traffic sources and destinations at the DHS TIC PEPs. The DHS CISO policy will prevent traffic as directed by the DHS CIO. 5.4.j – The DHS SOC shall oversee all enterprise PEPs. **Section 5.4.5 – Internet Security** – Prohibits Public Switched Telephone Network (PSTN) connection to OneNet. 5.4.5.a – Any direct connection of OneNet, DHS networks, or DHS mission systems to the Internet or to extranets shall occur through DHS Trusted Internet Connection (TIC) PEPSs. The PSTN shall not be connected to OneNet at any time. **Section 5.5.3 – Public Key/Private Key** – Assigns responsibility for non-human use of PKI to sponsors. 5.5.3.g – Sponsors for non-human subscribers (organization, application,

Version	Date	Description
		code-signing, or device) shall be responsible for the security of and use of the subscriber's private keys. Every sponsor shall read, understand, and sign a "DHS PKI Subscriber Agreement for Sponsors" as a pre-condition for receiving certificates from a DHS CA for the non-human subscriber. **Section 5.4.6 – Email Security** – Prohibits auto-forwarding of DHS email to other than .gov or .mil addresses. 5.4.6.i - Auto-forwarding or redirecting of DHS email to address outside of the .gov or .mil domain is prohibited and shall not be used. Users may manually forward individual messages after determining that the risk or consequences are low. **Section 5.4.7 – Personal Email Accounts** – Requires use of encryption when sending sensitive information to email addresses other than .gov or .mil addresses. 5.4.7.b - When sending email to an address outside of the .gov or .mil domain, users shall ensure that any sensitive information, particularly privacy data, is attached as an encrypted file. **Section 5.6 – Malware Protection** – Updates term from "Virus."
7.1	September 30, 2009	**General Updates** Standardized the term "IT system" to "information system" Standardized the term "DHS IT system" to "DHS information system" Updated the term "DHS Security Operations Center" to "DHS Enterprise Operations Center" and added definition in glossary Replaced "must" with "shall" in all policy statements Replaced "vendors" with "others working on behalf of DHS" **Specific Updates** **Section 1.4.20** – Strong Authentication – Added definition for Strong Authentication **Section 1.4.21** – Two-Factor Authentication – Added definition for Two-Factor Authentication **Section 2.2.4** – Component Chief Information Officer – Alleviated confusion regarding Component CIO responsibilities **Section 2.2.5** – Chief Security Office – Removed erroneous CSO responsibilities which belong to Component CIOs **Section 2.2.7** – DHS Chief Financial Officer – Updated policy elements to clarify applicable policies **Section 3.1** – Basic Requirements (3.1.d, 3.1.g-j) – Updated policy elements to CISO/ISSM/ISSO responsibilities **Section 3.7.f** – Clarified Operating system exception requirements **Section 3.9.l-m** – Clarified requirements regarding TAF/RMS **Section 3.15** – CFO Designated Systems – Major revisions to this section **Section 4.6.2 and 5.4.1.a** – Prohibits tethering to DHS devices

Version	Date	Description
		Section 5.4.3.g-h – Clarifies interconnection and ISA approval **Section 5.5** – Cryptography – Removed unnecessary elements from introductions and updated entire section with input from DHS PKI Steward
7.2	May 17, 2010	**General Updates** No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 1.4.8** – Added FISMA language (transmits, stores, or processes data or information) to definition of DHS System **Section 1.5.3.k** – Removed requirement for Component Head to make recommendation regarding waivers; removed requirement to report *exceptions* on FISMA report. **Section 2.1.6** – Adds requirement for AO to be a Federal employee **Section 2.1.7** – Clarifies that CO is a senior management official; stipulates that CO must be a Federal employee **Section 2.2.5** – Updated CSO role **Section 3.2** – Added intro to CPIC section and link to CPIC Guide **Section 3.5.2.h** – Added requirement to coordinate CP and COOP testing moderate and high FIPS categorizations **Section 3.15.a** – Added requirement for CFO Designated Systems security assessments for key controls be tracked in TAF and adds requirement for tracking ST&E and SAR annually. **Section 3.15.c** – Remaps control from RA-4 to RA-5 **Section 3.15.h** – Adds mapping to IR-6 **Section 3.15.i** – Remaps control from PL-3 to PL-2 **Section 3.17** – Added requirement to protect HIPAA information **Section 4.1.l.a** – Added requirement for annual reviews of position sensitivity levels **Section 4.1.1.c** – Exempts active duty USCG and other personnel subject to UCMJ from background check requirements **Section 4.1.4.c-d** – Adds additional separation of duties requirements and restricts the use of administrator accounts **Section 5.2.f** – Limits the number of concurrent connections for FIPS-199 high systems **Section 5.4.2.a** – Limits network monitoring as per the Electronic Communications Act **Section 5.4.3** – Added introduction to clarify ISA requirements **Section 5.4.3.f** – Clarifies the term "security policy" in context **Section 5.4.3.m** – Clarifies that both AOs must accept risk for interconnected systems that do not require ISAs. **Section 5.4.3.m-n** – Adds stipulations to ISA requirements

Version	Date	Description
		Section 5.5 – Updates language in entire section **Section 5.5.3.j** – Assigns the DHS PKI MA responsibility for maintaining Human Subscriber agreements
7.2.1	August 9, 2010	**General Updates** No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 1.1** – Removes reference to 4300C **Section 1.4.1/3** – Updates Executive Order reference from 12958 to 13526 **Section 1.4.17** – Updates the PII section **Section 1.4.18** – Updates SPII section **Section 1.5.3** – Adds requirement for Privacy Officer/PPOC approval for exceptions and waivers pertaining to Privacy Designated Systems **Section 1.6.b/c** – Requires installation and use of digital signatures and certificates **Section 2.1.6.d** – Allows delegation of AO duty to review and approve administrators **Section 2.2.6** – Updates DHS Chief Privacy Officer description **Section 3.7.e** – Adds requirement to include DHS certificate as part of FDCC **Section 3.14** – Updates Privacy and Data Security section **Section 3.14.1** – Updates PII section **Section 3.14.2** – Updates PTA section **Section 3.14.2.e** – Updates impact level requirements for Privacy Sensitive Systems **Section 3.14.3** – Updates PIA section **Section 3.1.4.4** – Updates SORN section **Section 3.14.4.a** – Exempts SORN requirements **Section 3.14.5** – Updates Privacy Sensitive Systems protection requirements **Section 3.14.6.a** – Updates privacy incident reporting requirements **Section 3.14.7** – Updates privacy requirements for e-Auth **Section 3.14.7.e** – Adds PIA requirements for eAuth **Section 4.1.1.e** – Expands U.S. citizenship requirement for access to all DHS systems and networks **Section 4.1.4.b** – Allows delegation of AO duty to review and approve administrators **Section 4.6.2.3.c** – Clarifies prohibited use of SMS **Section 4.8.4.h** – Updates the term “trusted” to “cleared” maintenance

Version	Date	Description
		personnel **Section 4.12.i** – Updates escort requirements for maintenance or disposal **Section 4.12.j** – Requires disabling of dial up on multifunction devices **Section 5.4.3** – Clarifies definition of Network Connectivity **Section 5.4.3.m/n** – Clarifies requirement for ISA **Section 5.4.6.j** – Requires DHS email systems to use a common naming convention **Section 5.5.3.g** – Prohibits sharing of personal private keys
7.2.1.1	January 19, 2011	**General Updates** No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 4.8.1.a** – Changes requirement for screensaver activation from five (5) to fifteen (15) minutes of inactivity.
8.0	March 14, 2011	**General Updates** Update date and version number Replace "certification and accreditation" and "C&A" with "security authorization process". Replace "Certifying Official" with "Security Control Assessor". Replace "ST&E Plan" with "security assessment plan". Replace "system security plan" with "security plan" and "SSP" with "SP". **Specific Updates** **Section 1.4.8.1:** Change definition to specify that a GSS has only one ISSO. **Section 1.4.8.2:** Change definition to specify that an MA has only one ISSO. **Section 1.5.1:** Include language requiring waiver submissions to be coordinated with the AO. **Section 1.5.2:** Include language requiring waiver submissions to be coordinated with the AO. **Section 1.5.3:** Clarify language regarding submission of waivers and exceptions for CFO designated systems. **Section 1.6.d:** Added new policy element, "DHS and Component systems shall be able to verify PIV credentials issued by other Federal agencies." **Section 2.1.2:** Add DHS CISO role as primary liaison to Component officials, and to perform periodic compliance reviews for selected systems. **Section 2.13:** Update Component CISO duties and add to implement POA&M process and ensure that eternal providers who operate information systems meet the same security requirements as the Component. **Section 2.1.4:** Update list of Component ISSM duties and create a POA&M

Version	Date	Description
		for each known vulnerability. **Section 2.1.5:** Add significantly expanded Risk Executive duties. **Section 2.1.6:** Add significantly expanded Authorizing Official duties. **Section 2.2.8:** Add Program Manager responsibility for POA&M content. **Section 2.2.9:** Add expanded System Owner duties. **Section 2.2.11:** Renumber 2.2.10 as 2.2.11. **Section 2.2.10:** Add a new 2.2.10 to introduce and describe duties of Common Control Provider. **Section 3.2.g:** Added new policy element, "Procurements for services and products involving facility or system access control shall be in accordance with the DHS guidance regarding HSPD-12 implementation." **Section 3.5.2.c:** Updated language to clarify requirements for backup policy and procedures. **Section 3.5.2.f:** Updated language to require table-top exercises for testing the CP for moderate availability systems. **Section 3.7.f:** Added new policy element, "Components shall monitor USGCB (or DHS-approved USGCB variant) compliance using a NIST-validated Security Content Automation Protocol (SCAP) tool." **Section 3.9:** Add requirement for Components to designate a Common Control Provider. **Section 3.10.b:** Policy element language was updated to clarify the function of information system security review and assistance programs. **Section 3.14:** Language updated for readability. **Section 3.14.c:** Added new policy element, "Components shall review and republish SORNs every two (2) years as required by OMB A-130." **Section 3.14.7.f:** Added new policy element, "Existing physical and logical access control systems shall be upgraded to use PIV credentials, in accordance with NIST and DHS guidelines." **Section 3.14.7.g:** Added new policy element, "All new systems under development shall be enabled to use PIV credentials, in accordance with NIST and DHS guidelines, prior to being made operational." **Section 3.17:** Added reference to NIST SP 800-66 for more information on HIPAA. **Section 4.1.4.d:** Language updated to clarify usage of administrator accounts. **Section 4.1.5.f:** Language updated to clarify requirements for security awareness training plan. **Section 4.3.1.b:** Language updated to clarify protection of offsite backup media. **Section 4.5.4:** Added reference to NIST SP 800-58 for more information on VoIP.

Version	Date	Description
		Section 4.9.j: Language updated to require that Component SOCs report operationally to the respective Component CISO. **Section 4.9.k:** New policy element added, "The DHS EOC shall report operationally to the DHS CISO." **Section 4.10:** Revise list of annual system documentation updates. **Section 4.12.c:** Policy element replaced with new one stating that the policy applies "to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS data." **Section 5.4.1.e:** Policy element removed. **Section 5.4.1.f:** Policy element removed. **Appendix A:** Include new acronyms **Appendix B:** Revise definition of Accreditation Package to reflect new list of documentation. **Appendix C:** Update references

Obama To Nominate A Defender For Whistle-Blowers

by Ari Shapiro

December 15, 2010

A federal office that ran aground under the Bush administration is about to get a new leader. The White House plans to nominate Carolyn Lerner to run the Office of Special Counsel, which represents federal whistle-blowers and other victims of discrimination within the government.

Whistle-blower groups applaud the nomination and call it long overdue.

"She's a great choice," says Debbie Katz, a private lawyer who represents government whistle-blowers. "She's going to have her work cut out for her."

Katz, who is familiar with Lerner's work, says the new special counsel "has a lot to do to restore credibility in this office, to make federal employees willing to go to that office with their complaints. The morale in that office is terrible now."

The morale problem is partly due to the tumultuous reign of the last head of the office, Scott Bloch. While the U.S. special counsel is supposed to serve a five-year term, Bloch never made it to the end of his term. He was removed from office at the end of the Bush administration and later pleaded guilty to withholding information from Congress.

"I gave a lot of credit to the career staff for being able to get their work done in the eye of Hurricane Scott," says Jim Mitchell, who was the office's spokesman until Bloch ousted him. "He became very defensive after the FBI raided the office."

That FBI raid in 2008 was part of an inquiry into whether Bloch erased files from his computer to obstruct a federal investigation. The investigation focused on whether Bloch had retaliated and discriminated against his employees.

An 'Extraordinary' Case

Danielle Brian of the Project on Government Oversight calls Bloch's tenure one of the most bizarre episodes in whistle-blower history. "Not only did he really not believe in the mission of the agency, but he was actually retaliating against his own employees, which is quite extraordinary, given that his job was to protect employees from this retaliation."

"As Special Counsel I made people on both sides mad," Bloch said in a written statement to NPR on Tuesday. "I made the Bush Administration mad by going after Karl Rove and making high ranking Republican officials leave office, causing 1000 planes to be grounded through investigations of the FAA, because that is the nature of the job."

Since the start of Bloch's tenure in 2004, whistle-blowers across the federal government have said they have had no good place to turn. "Literally hundreds of whistle-blowers every year who

can't afford a due process hearing or trial are defenseless when they try to defend the public against betrayals of trust," says Tom Devine of the Government Accountability Project. "They can be fired virtually at will, and if they go to the Office of Special Counsel, they'll be on an endless treadmill that goes nowhere."

The same is true of government workers fired for their race, gender, religion, sexual orientation or other protected classes. The Office of Special Counsel is supposed to stand up for them, but experts in the field say the office has been a dysfunctional shell for years now.

'Waiting For Godot'

Brian believes the White House's inaction — leaving the position vacant for two years — has had consequences. "The lack of strong legal protections for these employees is what is driving these people outside channels to the newspapers and to WikiLeaks," she says.

The Obama administration has taken steps to help whistle-blowers in other ways. The White House is pushing hard for a whistle-blower bill in Congress that now seems on the verge of passing. In light of that intense activity, government oversight groups were baffled that the president took so long to nominate someone to run the Office of Special Counsel.

"Frankly, I stopped asking, because how many times can you ask and hear, 'We're getting to it?' " said an exasperated Brian last week.

"It seems like we're waiting for Godot," added Devine of the Government Accountability Project.

Godot arrives with Lerner's nomination. She founded a civil rights and employment law firm in Washington, D.C., and she has worked on the sorts of retaliation and discrimination cases that characterize the workload of the Office of Special Counsel. She must be confirmed by the Senate before her five-year term can begin.

Quick Facts: Carolyn Lerner

The White House plans to nominate Carolyn Lerner to run the Office of Special Counsel.

- Lerner, who founded a civil rights and employment law firm in Washington, D.C., has worked on the sorts of cases that characterize the Office of Special Counsel's workload.
- Lerner is also an adjunct faculty member at George Washington University Law School, where she teaches mediation, and is a mediator for the U.S. District Court for the District of Columbia and the D.C. Human Relations Commission.
- Lerner's nomination must be confirmed by the Senate before she can begin a five-year term.

Source: NPR; Heller, Huron, Chertkof, Lerner, Simon & Salzman website

Heller, Huron is one of the premier employment law firms in the Washington, D.C. area. We represent individuals who believe their civil rights have been violated, or who need help with employment issues. The firm's expertise includes discrimination claims such as those based on sex or sexual harassment, hostile work environment, race, age, national origin, family responsibility, pregnancy, sexual orientation, military service and disability, as well as matters involving family and medical leave and retaliation. We litigate EEO claims under Title VII, ADEA, ADA, Rehabilitation Act, FMLA, Section 1981, USERRA and the D.C. Human Rights Act, as well as Maryland and Virginia civil rights statutes.

Our firm also advises organizations, non-profits and small businesses on compliance with employment laws; provides training; develops policies and employee handbooks; conducts sexual harassment investigations; mediates disputes; represents unions; and consults on a wide variety of employment matters. We provide advice and guidance for individual clients and organizations on other employment-related issues, such as non-compete agreements, employment contracts, executive compensation plans, and severance packages.

Our attorneys speak regularly at professional conferences and serve in leadership roles for various professional organizations, such as the Metropolitan Washington Employment Lawyers Association, the D.C. Bar, the Council for Court Excellence, and the Washington Council of Lawyers. The firm has been honored by the Washington Lawyers' Committee for Civil Rights with its Outstanding Achievement Award, and several of the firm's lawyers are recognized in *America's Best Lawyers* and *Washingtonian* magazine.

Our clients include a wide range of employees, such as government and private sector workers, hourly wage earners, corporate executives, salaried employees, and consultants, as well as unions and other organizations. We use our extensive experience and innovative advocacy to achieve fair and just results for our clients.

- Partners selected for Washington, D.C.'s 2011 *Best Lawyers*: Doug Huron, Carolyn Lerner and Richard Salzman for civil rights law; Stephen Chertkof, Doug Huron, and Richard Salzman for labor and employment law
- Richard Salzman speaks at D.C. Bar CLE program on sexual harassment cases

- Stephen Chertkof speaks at National Employment Lawyers Association 25th Annual Convention in a plenary session on defeating defendants' motions for summary judgment
- Doug Huron, who began his legal career in 1970 with the Employment Litigation Section of the Civil Rights Division of the Dept. of Justice, speaks at a conference at American University Law School celebrating the history and accomplishments of the Section
- Firm settles administrative assistant's race discrimination and retaliation case against the State Dept. for $275,000
- Firm obtains $200,000 judgment against the DOJ in pregnancy discrimination case
- Tammany Kramer joins the Board of the Metropolitan Washington Employment Lawyers Association and becomes Co-Chair of the MWELA Moot Court Committee
- Firm wins favorable ruling in Free Speech case for contractor fired for making peace video; 1st Amendment/discrimination

case against BBG/VOA to proceed. See *Daily Kos* coverage and video here.

- Firm settles race discrimination case against SBA for $160,000 plus promotion
- Firm wins at Supreme Court: case against U.S. senator goes forward
- *Washingtonian Magazine* recognizes firm partners as "Top Lawyers"
- Partners selected for America's Best Lawyers
- Firm wins ruling in retaliation claim against Giant Foods; case headed for trial
- Partners listed in D.C. Super Lawyers
- Firm settles federal employee retaliation case for $2.25 million
- Stephen Chertkof elected President of MWELA
- Carolyn Lerner becomes Board Chair of Center for Work Life Law
- Firm files *amicus* brief in Supreme Court retaliation case
- Douglas Huron named Lawyer of the Year
- $2 million jury verdict in federal employee "glass ceiling" case
- Betty Grdina serves as lead counsel in SEIU consumer class action

- $1.83 million settlement in race discrimination class action
- Co-counsel in largest ever sex discrimination settlement ($508 million)
- Co-counsel in landmark discrimination case brought by student against GW

1730 M Street, Suite 412, Washington, D.C. 20036 | (202) 293-8090 | Fax: (202) 293-7110

Possibly useful websites:

https://pubmini.dcma.mil/fraudnet/main.cfm

http://www.governmentfraud.us/pages/defense-contractor-fraud.php

http://www.defenselink.mil/faq/questions.aspx

http://www.dodig.osd.mil/HOTLINE/index.html

https://tips.fbi.gov/

http://www.ic3.gov/

http://www.ig.navy.mil/Contacts/Contact%20Us.htm

http://www.cnre.navy.mil/hotline/index.htm

http://www.jcs.mil/jcs_comment.html

http://www.navy.mil/submit/contacts.asp

http://www.pogo.org/p/x/exposecorruption.html

http://www.eeoc.gov/contact.html

http://www.false-claims-act.com/contact-us/

http://www.corpwatch.org/contactus.php

http://www.taf.org/

http://www.osha.gov/pls/osha7/eComplaintForm.html

http://www.usdoj.gov/oig/FOIA/hotline.htm

http://www.whistleblower.org/content/wsn.cfm

http://www.gao.gov/fraudnet/fraudnet.htm

http://www.fbi.gov/majcases/fraud/seniorsfam.htm

http://wikileaks.be/wiki/Wikileaks:Submissions

http://www.osc.gov/documents/forms/osc12.htm

http://www.ignet.gov/igs/homepage1.html#d

http://www.whistleblower.org/template/page.cfm?page_id=67

Resolution on WikiLeaks and Federal Agencies

WHEREAS, On December 3, 2010, the United States Office of Management and Budget issued an order blocking access to WikiLeaks across all federal agency networks;

WHEREAS, The Library of Congress blocked access to the WikiLeaks site from December 2 to December 7, 2010, across its computer systems, including those for use by patrons in its reading rooms;

WHEREAS, The Library of Congress has issued memos to its employees and posted signs in its reading rooms concerning applicable law, but unblocked its public access computers;

WHEREAS, The OMB order forbids federal employees access to WikiLeaks from their home computer systems and threatens punishment;

WHEREAS, OMB explained its actions by stating that applicable law obligates federal agencies to protect classified information and that unauthorized disclosures of classified documents do not alter the documents' classified status or automatically result in declassification;

WHEREAS, On matters of vital public concern, citizens' fullest knowledge and discussion are in the interest of democracy, freedom, peace, rule of law, and good governance here and around the world;

WHEREAS, Blocking access to published information is censorship, and supporting sanctions against reading is endorsing abridgment of intellectual freedom;

WHEREAS, The open publication of documents by WikiLeaks and other agencies of the free press renders the government classification status of these documents irrelevant; and

WHEREAS, The blocking of WikiLeaks curtails the public's right to know, violates the First Amendment of the Constitution of the United States, and fundamentally contradicts the principles of intellectual freedom as embodied in the Library Bill of Rights; now, therefore, be it

RESOLVED, That the American Library Association (ALA)

1. Calls for the amendment of Executive Order 13526, *Classified National Security Information* (December 29, 2009) to exclude publically available information;

2. Calls for the amendment of any other executive orders, public laws, or federal regulations that forbid access to publically available information; and

3. Calls for all US government agencies to follow the example of the Library of Congress concerning access to WikiLeaks.

Mover: Tiffani Connor, SRRT Councilor - trevellion70@yahoo.com

Seconder: Diedre Conkling, Councilor-at-Large - 541-961-3117

Sources:

1. OMB Memorandum: WikiLeaks - Mishandling of Classified Information. M 11-06, Nov. 28, 2010

   http://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-06.pdf

2. OMB's Model Memo To Federal Employees Banning Them From Wikileaks Site, No Date Given

   http://www.talkingpointsmemo.com/documents/2010/12/ombs-model-memo-to-federal-employees-banning-them-from-wikileaks-site.php?page=1

3. Why the Library of Congress Is Blocking Wikileaks, Dec. 3, 2010
   http://blogs.loc.gov/loc/category/news/

4. Memo: Library of Congress and Access to WikiLeaks Website, Dec. 21, 2010

   On December 2, upon learning of the possibility that classified documents could be accessed on Library of Congress systems that are not authorized for classified information, the Library temporarily blocked access to the WikiLeaks website on Library premises.

   The Library publicly announced this block, in response to news requests, on December 3, stating “The Library decided to block WikiLeaks because applicable law obligates federal agencies to protect classified information. Unauthorized disclosures of classified documents do not alter the documents’ classified status or automatically result in declassification of the documents.”

   Since that time, the Library has reminded its employees and patrons of their responsibility to comply with laws regarding classified information, regardless of whether the information appears on WikiLeaks or another site, and has developed protocols to protect its systems:

   * A notice went out to all employees with security clearances on December 3.

   * An LC Operations Announcement went out to all employees December 7.

   * A notice is to be posted in all reading rooms, preferably at the point where researchers sign in.

   With these protections in place, the Library unblocked the WikiLeaks website, beginning on December 7, and is not currently monitoring access to that site.

December 21, 2010

Congressional Research Service

Report 98-691

LEGAL ANALYSIS OF E.O. 13087 TO PROHIBIT DISCRIMINATION BASED ON SEXUAL ORIENTATION IN FEDERAL EMPLOYMENT

Charles V. Dale, American Law Division

Updated August 14, 1998

Abstract. E.O. 13087, issued by President Clinton on May 28, 1998, amends a nearly 30-year executive order, E.O. 11478, to prohibit sexual orientation discrimination in most federal civilian employment along with other forms of bias covered by the earlier order.

CRS Report for Congress

Legal Analysis of E.O. 13087 to Prohibit Discrimination Based on Sexual Orientation in Federal Employment

August 14, 1998

Charles V. Dale
Legislative Attorney
American Law Division

Abstract

E.O. 13087, issued by President Clinton on May 28, 1998, amends a nearly 30-year executive order, E.O. 11478, to prohibit sexual orientation discrimination in most federal civilian employment along with other forms of bias covered by the earlier order.

Legal Analysis of E.O. 13087 to Prohibit Discrimination Based on Sexual Orientation in Federal Employment

Summary

E.O. 13087 amends a nearly 30 year-old executive order, E.O. 11478, to prohibit sexual orientation discrimination in most federal civilian employment along with the other forms of bias covered by the earlier order. The nondiscrimination and "affirmative program of equal employment opportunity" requirement of the executive order extends to "every aspect of personnel policy and practice in employment, development, advancement, and treatment of civilian employees of the federal government." It applies to civilian employment by the executive branch, including the military departments, and sundry other agencies but does not cover the uniformed military. In addition, although it purports to apply to legislative and judicial branch entities "having positions in the competitive service," relatively few such positions exist outside the executive branch, and E.O. 11478 has been judicially held not to apply to noncompetitive and excepted service personnel. This report will be updated as events warrant.

Legal Analysis of E.O. 13087 to Prohibit Discrimination Based on Sexual Orientation in Federal Employment

On May 28, 1998, President Clinton issued an amendment to E.O. 11478 which states a basic policy of equal employment opportunity in federal executive branch departments and agencies. The original order, as earlier amended, prohibits discrimination because of "race, color, religion, sex, national origin, handicap, and age" in covered employment and requires each executive department and agency to promote equal opportunity through a "continuing affirmative program." The scope of the equal opportunity mandate in E.O. 11478 encompasses "every aspect of personnel policy and practice in employment, development, advancement, and treatment of civilian employees of the federal government." The Clinton order, E.O. 13087, adds "sexual orientation" after "age" as a protected category in Section 1 of the underlying document along with qualifying language, in effect, authorizing the expansion of coverage only "to the extent permitted by law."

The nature of the nondiscrimination and other obligations imposed on federal departments and agencies by E.O. 11478 is spelled out in some greater detail in Section 2. Thus, each agency head must establish and maintain an "affirmative program of equal employment opportunity" for all civilian employees and applicants emphasizing active outreach and recruitment efforts; employee development and training designed to fully utilize and "enhance" employee skills and advancement opportunities to "their highest potential;" training for managers and supervisors to promote "understanding and implementation" of the policy; and a system for oversight and periodic evaluation of program effectiveness. Beyond these more or less inward-looking aspects of the program, federal managers are also directed to "assure participation at the local level with other employers, schools, and public or private groups in cooperative efforts to improve community conditions which affect employability . . ." The Equal Employment Opportunity Commission has overall responsibility for implementing the executive order program through the issuance of rules and regulations which are binding on federal departments and agencies.[1]

When Title VII of the Civil Rights Act of 1964 was enacted, federal employees were not protected since the federal government was specifically excluded from the definition of an "employer" covered by the Act. Section 701 did, however, provide

---

[1] Section 4 of E.O. 11478 directs the EEOC to "carry out" the order through the issuance, "after consultation with all affected departments and agencies," of "such rules, regulations, orders, and instructions . . . as it deems necessary and appropriate" and the head of each employing agency is required by § 5 to furnish the Commission with reports and information as requested and to "comply with rules, regulations, orders, and instructions" issued by it.

that federal sector employment decisions were to be free from discrimination. The President was authorized to issue executive orders enforcing this policy. "*Provided further,* That it shall be the policy of the United States to insure equal employment opportunities for federal employees without discrimination because of race, color, religion, sex or national origin and the President shall utilize his existing authority to effectuate this policy."[2] To carry out this mandate, President Nixon issued E.O. 11478 in 1969, replacing portions of an earlier Johnson Administration directive on the subject.[3] Pursuant to the order, the former Civil Service Commission established comprehensive administrative procedures for the investigation and resolution of discrimination complaints by federal employees. However, the courts from an early date denied a right to judicial review of discrimination claims brought pursuant to the executive order.[4]

The lack of a judicial remedy for federal employees was rectified in 1972 when Congress extended Title VII coverage to the federal workplace and provided for *de novo* review in federal court of federal employee discrimination claims following completion of the administrative process. Explicit congressional ratification of the E.O. 11478, as then written, was included in § 717(c) of the 1972 amendments which authorized private civil actions for federal employees complaining of "discrimination based on race, color, religion, sex, or national origin." In addition, the amendments state:

> Nothing contained in this Act shall relieve any Government agency or official of its or his primary responsibility to assure non-discrimination in employment as required by the Constitution and statutes or of its responsibilities under Executive Order 11478 relating to equal employment opportunity in the Federal Government.[5]

The Civil Service Commission's responsibility for enforcing Title VII and the Executive Order was transferred to the EEOC pursuant to Reorganization Plan No. 1 of 1978 and the Civil Service Reform Act of 1978. The EEOC carried forward the Commission's regulatory enforcement scheme, which was incorporated into the EEOC's overlapping statutory jurisdiction.

The EEOC regulations elaborate upon the responsibility of federal departments and agencies for maintaining an "affirmative program" of equal employment opportunity as required by § 717 and the Executive Order. Aside from procedures for processing complaints of discrimination, those rules focus on two major aspects of a federal employer's compliance with nondiscrimination requirements. First, they make clear that the equal opportunity mandate extends to all of a department or agency's "personnel policies, practices, and working conditions"--including job advertising, recruitment, training activities, promotion, discipline and discharge, etc. Secondly, the regulations emphasize the need for measures to inform and educate other employees, supervisors and managers in particular, concerning their role in

---

[2] P.L. 88-352, § 701(b), 78 Stat.241, 252 (1964).

[3] E.O. 11246, 30 Fed. Reg. 12319 (1965).

[4] See e.g. Gnotta v. United States, 451 F.2d 1271 (8th Cir. 1969), cert. denied, 397 U.S. 934 (1970); Brown v. G.S.A., 425 U.S. 820 (1976).

[5] 42 U.S.C. 2000e-16(e).

program implementation. Thus, the governmental employer is to "enlist th[e] cooperation" of the agency's general workforce and labor organizations and must take "appropriate disciplinary action" against discriminating employees. Similarly, managers and supervisors are to be provided "orientation, training, and advice" on the program with their participation being a factor in the evaluation of their job performance.

Both Executive Order 11478, and the EEOC regulations described above, make plain that the mandated "affirmative program of equal employment opportunity" is to encompass "every aspect of personnel policy and practice," including "recruitment activities," and that systems are to be established for "periodically evaluating the effectiveness of the agency's overall equal employment opportunity effort."[6] The scope of this legal obligation, and specific initiatives adopted by federal agencies to implement it, have received scant judicial attention, perhaps because the order was so soon supplanted by statutory amendment to Title VII. A corollary legal requirement was incorporated into § 717 of the 1972 Title VII amendments, which requires each federal department and agency to submit for annual EEOC review "an affirmative program of equal employment opportunity" for all employees or applicants for employment.[7] The statute, however, has since 1978 been administered jointly with a provision of the Civil Service Reform Act, which authorized a federal "minority recruitment program" designed to eliminate "underrepresentation" of racial and ethnic minorities, and women, in specific job categories.[8] That program has no application to sexual orientation -- just as it does not extend to older workers and religious minorities who are also protected by E.O. 11478.

On account of this statutory history, minority and female recruiting practices of federal agencies provide no direct guidance to interpreting E.O. 11478 as most recently amended. E.O. 13087 does not explicitly mandate affirmative recruitment or other preference in federal employment based on sexual orientation. But neither does it or other legal authority preclude federal employing departments and agencies from incorporating statistically--based measures into an overall "affirmative program of equal employment opportunity." Determination of administrative policy in this regard would appear to be within the discretion of individual departments and agencies under § 2 of E.O. 11478. In addition, under §§ 4 and 5 of E.O. 11478, as amended, EEOC would arguably have the authority, but not a legal duty, to require recordkeeping by agencies of workforce composition based on sexual orientation.[9]

---

[6] 29 C.F.R. §1614.102(a)(11).

[7] 42 U.S.C. § 2000e-16(b)(1).

[8] The EEOC and Office of Personnel Management have issued rules to guide monitoring and compliance of minority recruitment programs adopted by individual federal agencies, including the requirement of "annual specific determinations of underrepresentation for each group . . . accompanied by quantifiable indices by which progress towards eliminating underrepresentation can be measured." 5 C.F.R. § 720.205(b)(1998).

[9] EEOC regulations issued pursuant to E.O. 11478 and the 1972 Title VII amendments require covered departments and agencies "to collect and maintain accurate employment information on the race, national origin, sex and handicap(s) of its employees" by means of "voluntary self-identification" and to report on same to the Commission "in such form and

(continued...)

Note, however, that neither affirmative recruitment nor data collection appear to be required by agency practice with respect other classes protected by E.O. 11478--older workers and religious minorities, for example--leaving the prospects for future agency action on sexual orientation largely conjectural.

The effect of the Clinton Administration order on federal health insurance, family leave, and other employment benefits for federal employees that include marital status distinctions would probably be marginal. Definitional aspects of family relationship, i.e. husband, wife, spouse etc., required for participation in most such programs are set by statute.[10] Thus, any claim of sexual orientation discrimination resulting from the denial of benefits to any person not the spouse or child of an employee--or an agency's voluntary adoption of domestic partnership policies-- would for many federal purposes be contrary to law and outside the scope of E.O. 13087. But in light of the U.S. Supreme Court ruling last term in *Oncale v. Sundowner Offshore Services Inc.*[11]-- finding that Title VII prohibits same-sex harassment-- the new order could require agencies to take actions to prevent and remedy harassment of employees based on their sexual orientation. Such anti-harassment policies could include agency-sponsored training programs to foster awareness and appreciation of diversity in matters of sexual orientation. Employees objecting to compulsory attendance at such programs on moral or religious grounds may enjoy uncertain constitutional protection.[12] However, objectors might in some circumstances find relief in the EEOC regulations which require agencies to "reasonabl[y] accommodate" the religious needs of employees when this can be done without "undue hardship" to agency business.[13] Nor would the amended order necessarily preclude even-handed application to all employees, regardless of sexual orientation, of agency rules governing employee conduct in relation to displays of affection or other workplace behavior that could "reasonably be expected to interfere with, or prevent, effective accomplishment by the employing agency of its duties and responsibilities."[14]

The executive order has its most obvious and direct implication on federal employers and for the rights of employees and applicants for employment in the Executive Branch. It would not immediately impact the employment practices of federal contractors--who are subject to nondiscrimination and affirmative action requirements on the basis of race, ethnicity, and gender imposed by E.O. 11246--or recipients of federal financial assistance governed by a host of other nondiscrimination statutes which do not include sexual orientation protections.

---

[9](...continued)
at such times as the Commission may require." 29 C.F.R.§ 1614.602 (a),(b), and (g).

[10] E.g. the Federal Employee Health Benefits Plan defines "member of the family" to include the "spouse" of an employee and an "unmarried dependent child." 5 U.S.C. § 8901; "Spouse" for purposes of the Family and Medical Leave Act, 29 U.S.C. § 2611(13) means "husband or wife, as the case may be."

[11] 118 S.Ct 998 (1998).

[12] Cf. Roberts v. United States Jaycees, 468 U.S. 509 (1984)(rejecting First Amendment challenge to state law forcing a nominally "members-only" association to admit women to its all-male ranks).

[13] 29 C.F.R. § 1614.102(a)(7).

[14] 5 C.F.R. § 731.202(a)(2).

Nonetheless, it is possible that E.O. 11478, as amended, could have ramifications for the private sector. In addition to internal measures to avoid discrimination and affirmatively enhance employment opportunities within the agency, federal employers are directed to engage in "cooperative efforts" with employers, schools, and public or private groups "at the local level" in aid of these objectives. The authority to cooperate with local entities could conceivably provide a basis for requiring or encouraging the adoption of sexual orientation policies by such entities as a condition to federal cooperation. Some parallel may be found in federal regulations unrelated to E.O. 11478 which have either mandated nondiscrimination or required the affirmative consideration of sexual orientation as a criterion by participants in other federal programs.[15] It appears, therefore, that the sexual orientation amendment to the executive order program could have at least some policy implications outside the federal workplace.

The ability of federal employees or applicants to complain of and obtain administrative relief for alleged sexual orientation discrimination under the amended executive order may largely depend on future rule-making by the employing federal departments and agencies and/or the EEOC. Current procedures for enforcing equal employment opportunity with respect to other classes of employees protected by E.O. 11478 are established by EEOC regulations. Briefly, a federal employee aggrieved by discrimination must first consult with an agency EEO counselor for advice and informal resolution of the matter which, if unsuccessful, may be followed by a formal complaint with the employing agency, an investigation, and ultimately a hearing before an EEOC administrative law judge. Any final agency determination may be appealed to the EEOC and from there to the federal courts in racial, ethnic, religious, or gender discrimination cases. A right to judicial review in sexual orientation cases would not be independently available under the executive order without congressional authorization.

In addition, an argument could be made that because E.O. 13087 adds "sexual orientation" only to the statement of policy in § 1, but not the more explicit "implementation" language in § 3, the employing departments and agencies, rather than the Commission, may be primarily responsible for determining procedures for administrative enforcement. A signing statement issued by the President on May 28 possibly suggests such intent when it declares that "[t]his Executive Order [13087] does not and cannot create any new enforcement rights (such as the ability to proceed before the Equal Employment Opportunity Commission) . . ." Clouding the issue further, however, is the fact that the Commission's current authority under § 4 of E.O.

---

[15] E.g. 61 Fed. Reg. 40380, 40388 (8-2-96)(private participants in Groundfish Observer Program "must assign observers without regard to any preference by representatives of vessels and shoreside facilities based on observer race, gender, age, religion, or sexual orientation"); 60 Fed. Reg. 20684, 20692 (4-27-95)(applicants for Runaway and Homeless Youth Program must identify strategies "for encouraging awareness of and sensitivity to the diverse needs of runaway and homeless youth who represent particular ethnic and racial backgrounds, sexual orientations, or are street youth"); 46 Fed. Reg. 18055, 18056 (legal services programs supported by Legal Services Corporation may not discriminate on the basis of sexual orientation in delivery of legal services and "must take affirmative action to end the underutilization of certain protected groups in their workforces"); 59 Fed. Reg. 96599 (3-28-94) (Americorps technical training and assistance to state commissions or alternative entities to include "developing strategies which encourage mutual respect and cooperation among citizens of different . . . sexual orientations ").

11478 "to issue such rules, regulations, orders, and instructions, and request such information from the affected departments and agencies as it deems necessary and appropriate" remains intact. In any event, while E.O. 13087 may not create enforcement rights (and only Congress can create a judicial right of action by statute), the employing agencies and the EEOC share a residuum of rulemaking authority under E.O. 11478, which could arguably be deployed to procedurally implement the order at the administrative level.

Another enforcement avenue may exist, however. The Office of Special Counsel (OSC) was created by the Civil Service Reform Act to investigate allegations of "prohibited personnel practices" within the executive branch and, when appropriate, to seek corrective and disciplinary action through auspices of the Merit System Protection Board (MSPB).[16] Falling within the independent investigatory jurisdiction of the OSC is any allegation of "activities prohibited by any civil service law, rule, or regulation" and "involvement by an employee in any prohibited discrimination found by any court or appropriate administrative authority to have occurred in the course of any personnel action." [17] Allegations of sexual orientation discrimination prohibited by E.O. 13087 may come within this definition. OSC has no independent enforcement authority, however, but where it finds "reasonable grounds," may seek stays and corrective action from the MSPB against the employing agencies and disciplinary sanctions against alleged discriminators.

Questions have arisen as to whether any statutory basis exists for the most recent amendment to E.O. 11478 regarding sexual orientation discrimination. While Congress has authorized and approved of the executive order program as applied to racial minorities and women, both before and after its implementation, the legislative history of Title VII and the 1972 amendments provides negligible support for the post-enactment revisions effected by E.O. 13087. The President does, however, possess executive authority under the federal civil service laws to make such rules "as will best promote the efficiency of [the] service." Thus, 5 U.S.C.§ 3301 provides:

> The President may---
> (1) prescribe such regulations for the admission of individuals into the civil service in the executive branch as will best promote the efficiency of that service;
> (2) ascertain the fitness of applicants as to age, health, character, knowledge, and ability for the employment sought;
> (3) appoint and prescribe the duties of individuals to make inquiries for the purpose of this section.

In addition, while the Civil Service Reform Act of 1978 does not mention "sexual orientation," it incorporates a job-based performance standard which has been administratively interpreted since the Carter Administration as barring disqualification of persons from the federal service based on sexual orientation alone.[18] By 1996, at least thirteen cabinet level agencies and 33 independent

---

[16] 5 U.S.C. § 1212.

[17] Id., § 1216(a)(4),(5).

[18] 5 U.S.C. § 4302(b)(1)("performance standards" to be based on "objective criteria. . .related to the job in question for each employee or position. . ."). See also "Federal (continued...)

establishments of the U.S. Government had reportedly issued policy statements forbidding sexual orientation discrimination. These included the Departments of Justice (including the FBI), Agriculture, Transportation (including the Coast Guard), Health and Human Services, Interior, Housing and Urban Development, Labor, Energy and the General Accounting Office, General Services Administration, Internal Revenue Service, Office of Personnel Management, the White House, and the Federal Reserve System.[19] E.O. 13087 essentially makes such policy universal in the Federal Executive Branch and with respect to civilian employees of the military departments and sundry other governmental entities, but would not create judicially enforceable rights in the absence of congressional action.

On August 5, 1998, the House , by a vote of 176 to 252, defeated a floor amendment offered by Representative Hefley to H.R. 4276, the FY 1999 Commerce, Justice, State appropriations measure, that would have prohibited the use of appropriated funds to implement or enforce E.O. 13087.[20].

---

[18](...continued)
Employees Gain Better Protection Against Sexual Orientation Discrimination," 24 DLR (BNA) A-9 (Feb. 7, 1994)(citing 1980 Office of Personnel Management memorandum explaining that sexual orientation discrimination is illegal.)

[19] See Serra, "Sexual Orientation and Michigan Law," 76 Mich. B.J. 948, 949 (1997).

[20] 144 Cong. Rec. H7263 (daily ed. 8-5-98).

Reference: Luskin, B. J. (Autumn 2011). Whistleblowing is a Tricky Business. Work Style Magazine, 16-17.

A worldwide observatory on work style changes

Work Style Magazine

Editorial by Bernard Luskin

Whistleblowing is a Tricky Business

A Whistleblower can be an individual who outs or opines practices or actions that are illegal, dishonest or violate the whistleblower's sense of morality or ethics. There are many new protections to guard the messenger in order to prevent the whistleblower from ending up as the victim.

Illustration by Goñi Montes, Decatur, USA

Whistleblowing is one of the most effective means used for continuously monitoring of individuals and to ensure that managers follow procedures.

Whistleblowers

In 1864, the US Congress passed the "False Claims Act" that was first signed into law by Abraham Lincoln during the Civil War. The act allowed an individual to file suit on behalf of the United States against anyone committing fraud impacting the federal government. This is an example of an early vehicle that provided a whistleblower some protection and encouraged them

to report sensitive information. The record of many whistleblowers is reflected in the reporting of dishonest or fraudulent acts within their organizations or businesses. There are also people who blow the whistle on other individuals or organizations in which they do not work but are given incentives to report and expose illegal, dishonest or socially unacceptable acts. US Qui Tam rules also encourage whistleblowers to report issues while rewarding them with a percentage of money recovered by the government as an outcome of a legal case.

WHAT PERSONALITY TYPE ENABLES A PERSON TO WILLINGLY REPORT A FELLOW EMPLOYEE, SUPERIOR, INDIVIDUAL OR GOVERNMENT AGENCY KNOWING THERE WILL BE CONSEQUENCES?

Some people would call them courageous or even heroes in instances that uncover and expose an injustice. However, one risk is that a whistleblower may become a target for retaliation. So, there must be a genetic risk propensity in the brain wiring of the whistleblower. Included in the risk is the possibility of a negative stigma, such as "Tattletale." This possibility requires a willingness to confront adversity. Whistleblowers show up in the news often and capture our collective attention. Movies or news reports cover their lives. The most recent example is the independent movie The Whistleblower which is being released now and may be nominated for an Oscar. Other examples of famous public whistleblowers include Daniel Ellsberg and the Pentagon Papers, Jeffrey Wigand and the tobacco industry, Karen Silkwood and the nuclear industry, Cynthia Cooper and Sherron Watkins who exposed Enron2 and Julian
Assange, the whistle-blower who created an organization and website called WikiLeaks, 3." The results are inconclusive at the moment and the motivation of the leakers are debatable. Julian Assange is a highly visible public figure and was the runner up

for Time Magazine's Person of the Year with readers voting 1,249,425 times for the Australian-born self-proclaimed crusader of truth and reform4. He has a strong opinion of right and wrong and possesses the dedication to continue releasing controversial information.

IS JULIAN ASSANGE A "WHISTLEBLOWER" OR IS HE A JOURNALIST WHO HAS CREATED A FORUM FOR WHISTLEBLOWERS?

Assange has not personally blown the whistle, yet he has published confidential papers that others have obtained and have given to Assange for his publication. Is he a heroic figure, a shrewd business-man or a thrill seeking exhibitionist? He may be a Pied Piper of whistleblowing, a Rupert Murdoch of the new journalism or something else? Because of the controversial nature of Assange's case, it is hard to classify him with a standard whistleblower's psychological profile but I do list some general insights.

My years as a psychotherapist lead me to offer the following information about the traits of a typical whistleblower:

Whistleblowers:

· are driven by altruism.
· can overcome insecurity through exhibitionism in order to release information.
· are generally moralistic, becoming committed and even obsessed about a personal belief.
· have a propensity to rely on moral theories that emphasize rights.
· are strong willed.
· are stubbornly committed and uncompromising.
· are willing to go against social conventions.

· rely on their own attitudes and beliefs.
· come from a mindset.

In most cases, society determines the right and wrong of social issues. Illegal or criminal exposure takes whistleblowing to another level. However, in my experience, altruism, a personally defined morality, rigidity and strong will, a willingness to counter social conventions and rely on one's own beliefs, are the general characteristics of an individual with a propensity to expose controversial events and information. There are many lists of personality types that may apply. Some lists include an idealist, protector, visionary, enforcer, and do-gooder. In the public arena, there have been a number of high profile whistleblowers in recent years and many share a number of the personality characteristics I have described. No doubt the psychological
profile of a whistleblower captures the public's imagination and is helpful to know for both industry and government. It is therefore important to understand this personality regardless of a person's or institution's opinion on the action of whistleblowing itself. Touro University Worldwide online master's degrees include various disciplines and courses that investigate the psychology of whistleblowers and other psychological profiles, which impact Human Resource issues and business in general.

ABOUT THE AUTHOR
Bernard Luskin, EdD, LMFT, is CEO, Senior Provost and Professor of Marriage and Family Therapy at Touro University Worldwide (www.TouroW.edu). Dr. Luskin received the 2011 American Psychological Association Media Psychology Division Life Achievement Award for contributions to Media Psychology. He was Co-Director of the APA Task Force Report on Psychology and New Technologies and was founder of the first PhD program in Media Psychology in any university while serving as professor of psychology at Fielding Graduate University.

Contact Dr. Luskin at Bernard.Luskin@TouroW.edu.

Magazine Link: http://theworkstylemagazine.byway.it/nl/f.jsp5K.Jb.EET.h.P.vJfq
TUW Link: http://www.TouroW.edu

###

WHISTLEBLOWERS AND THE OBAMA PRESIDENCY: THE NATIONAL SECURITY DILEMMA

BY
RICHARD MOBERLY*

* Professor of Law, University of Nebraska College of Law. I appreciate the helpful comments from Jack Beard, Eric Berger, Steve Bradford, Susan Poser, Kevin Ruser, Robert Vaughn, Steve Willborn, the participants at the Sixth Annual Labor and Employment Law Colloquium at Southwestern Law School in Los Angeles, CA, and the faculty at the Nebraska College of Law who attended a colloquium presentation of this paper. Caleb Dutson, Ryan Sullivan, and Nick Thielen provided excellent research assistance. A McCollum Research Grant provided support for the research and writing of this article. In 2008, I served on two Obama for President Expert Policy Committees: the Government Reform Policy Committee and the Labor and Employment and Workforce Policy Committee; however, I did not provide advice on national security whistleblower policy and the opinions expressed herein are my own.

I. INTRODUCTION

Whistleblower advocates generally cheered Barack Obama's election in 2008 because they had a "longtime friend" ascending to the Presidency.[1] Before entering public service, Obama represented a qui tam whistleblower as an attorney, and then, as both a state senator and a U.S. senator, Obama supported whistleblower protection legislation.[2] As a candidate for President, Obama reiterated his support for expanded whistleblower protections.[3] Most importantly, as President-Elect, Obama promised to reinvigorate ethics in government, and part of his plan included increased protections for whistleblowers. Before he took office, the Obama-Biden transition team stated,

> [o]ften the best source of information about waste, fraud, and abuse in government is an existing government employee committed to public integrity and willing to speak out. Such acts of courage and patriotism, which can sometimes save lives and often save taxpayer dollars, should be encouraged rather than stifled. We need to empower federal employees as watchdogs of wrongdoing and partners in performance. Barack Obama will strengthen whistleblower laws to protect federal workers who expose waste, fraud, and abuse of authority in government. Obama will ensure that federal agencies expedite the process for reviewing whis-

1. Joe Davidson, *Joe Davidson's Federal Diary: Whistleblowers May Have Friend in Oval Office*, WASH. POST, Dec. 11, 2008, at D3; *see also* TOM DEVINE & TAREK F. MAASSARANI, THE CORPORATE WHISTLEBLOWER'S SURVIVAL GUIDE 183 (2011) ("The Obama Administration's arrival brought high expectations that times are, indeed, a-changin'."); Megan Chuchmach & Rhonda Schwartz, *Will Obama Keep His Promise to Federal Whistleblowers?*, ABC NEWS (Aug. 4, 2009), <http://abcnews.go.com/Blotter/story?id=8241580&page=1>.

2. Chuchmach & Schwartz, *supra* note 1; Davidson, *supra* note 1.

3. Letter from Barack Obama to The National Academies (Oct. 9, 2008), *available at* <obama.3cdn.net/08fe869a2e4de42af1_zam6b5vn2.pdf> ("I will strengthen protections for 'whistleblowers' who report on any government attempts to distort or ignore scientific research.").

tleblower claims and whistleblowers have full access to courts and due process.[4]

In many ways, President Obama has lived up to his promised support for whistleblowers. Obama's appointments to key administrative positions in charge of whistleblower protection consistently supported employee rights and worked steadily to unravel the long-standing anti-whistleblower bias in those agencies.[5] Moreover, the three most prominent pieces of Obama's legislative agenda – the economic stimulus package, the financial reform bill, and health care reform – all included key provisions that enhanced whistleblower protections.[6]

However, the Obama Administration's record regarding whistleblower protection for *national security* whistleblowers has been decidedly less emphatic and more nuanced.[7] Indeed, the Obama Administration has been accused of conducting a "war on whistleblowers," because of its aggressive prosecution of leaks related to national security.[8] Obama's Department of Justice (DOJ) prosecuted six people who allegedly disclosed sensitive information to non-governmental entities (such as the media) under the Espionage Act, a statute typically used to prosecute disclosure of national secrets to foreign governments – more such prosecutions than all previous administrations combined.[9] Moreover, Obama's Administration has continued the Bush Administration's attempts to coerce reporters into identifying the sources of national security leaks.[10] Further, his support for statutory improvements to antiretaliation laws varies depending on whether the

4. *Agenda · Ethics*, CHANGE.GOV <http://change.gov/agenda/ethics_agenda/> (last visited Apr. 16, 2012).

5. *See* discussion *infra* Part II.A.1.

6. *See* discussion *infra* Part II.A.2.

7. *See* Jane Mayer, *The Secret Sharer*, THE NEW YORKER, May 23, 2011, at 47, 48 (asserting that President Obama has drawn a "sharp distinction between whistle-blowers who exclusively reveal wrongdoing and those who jeopardize national security").

8. Glenn Greenwald, *The DOJ's Creeping War on Whistle-Blowers*, SALON (Feb. 25, 2011, 7:26 AM CDT), <http://www.salon.com/2011/02/25/whistleblowers_4/>; Scott Horton, *Obama's War on Whistleblowers*, HARPER'S MAGAZINE (Aug. 31, 2010, 1:33 PM), <http://www.harpers.org/archive/2010/08/hbc-90007562>; *see also* Conor Friedersdorf, *The Obama Administration's Whistleblower Problem*, THE ATLANTIC (June 30, 2011, 7:10 AM ET) <http://www.theatlantic.com/politics/archive/2011/06/the-obama-Administrations-whistleblower-problem/241262/> (noting that the Obama Administration, "for reasons big and small, fair and possibly unfair, . . . has acquired a reputation for retaliating against whistleblowers"); Josh Gerstein, *Justice Dept. Cracks Down on Leaks,* POLITICO (May 25, 2010, 4:44 AM EDT) <http://www.politico.com/news/stories/0510/37721.html> ("President Barack Obama's Justice Department has taken a hard line against leakers, and Obama himself has expressed anger about disclosures of national security deliberations in the press.").

9. Charlie Savage, *Ex-C.I.A. Officer Charged in Information Leak*, N.Y. TIMES, Jan. 23, 2012, at A1; Scott Shane, *U.S. Pressing Its Crackdown Against Leaks*, N.Y. TIMES, June 18, 2011, at A1; discussion *infra* Part II.B.2.

10. *See* discussion *infra* Part II.B.2.

proposed protection affects whistleblowers in the intelligence community.[11]

This Article explores President Obama's seemingly contradictory approach to whistleblowers and the distinction he appears to draw between whistleblowing about governmental misconduct generally, which he supports, and whistleblowing in the national security context, which he appears to disdain. Part II of the Article describes the numerous moves Obama made to improve whistleblower protection through his Presidential appointments and his support of improved antiretaliation statutory measures. Additionally, this Part contrasts that support with Obama's seemingly antagonistic approach to whistleblowing about national security.

At least two questions arise from drawing this distinction between national security whistleblowing and other types of whistleblowing. First, where does the distinction come from? Second, does the distinction make sense?

Part III answers the first question by examining why Obama might approach national security whistleblowing differently than other types of whistleblowing. In some respects, this different approach continues a long-standing separation of powers dispute between the legislative and the executive branches of the federal government. Congress desires transparency and oversight of the executive branch, which it hopes to achieve by encouraging executive branch employees to disclose information to Congress. Presidents traditionally have resisted these efforts, particularly when they involve matters over which the Constitution arguably has empowered the President with exclusive domain, such as protecting secrecy related to national security. The state of the law related to national security whistleblowers reflects this dispute in that such whistleblowers generally receive far fewer protections than other types of whistleblowers. In short, President Obama values secrecy over transparency and oversight when it comes to national security whistleblowing, and the law often reflects and supports this choice.

Part IV responds to the second question – does this distinction make sense? – by analyzing whether President Obama and the current state of the law correctly balance the competing goals of secrecy and security on the one hand and transparency and oversight on the other. Although reasons certainly exist to treat national security whistleblowers differently than other whistleblowers, I argue in this Part that the law could be modified to increase transparency and oversight without a corresponding negative impact on secrecy and national security. I conclude the Article with several sug-

11. *See id.*

gestions to re-balance the scales and to provide national security employees appropriate encouragement to blow the whistle on governmental misconduct.

II. OBAMA'S NUANCED APPROACH TO WHISTLEBLOWING

> Every government has an interest in concealment; every public, in greater access to information. In this perennial conflict, the risks of secrecy affect even those administrators least disposed at the outset to exploit it. How many leaders have not come into office determined to work for more open government, only to end by fretting over leaks . . . .
>
> *Sissela Bok (1982)*[12]

A. Obama's Support for Whistleblowers Generally

In several important respects, President Obama has supported whistleblowers as he promised during the campaign.

1. Presidential Appointments

First, President Obama appointed supporters of whistleblower rights to key administrative positions involved in protecting whistleblowers.[13] At least one whistleblower advocate felt that Obama's appointments were "a weathervane that the Obama Administration is serious about its good government rhetoric."[14] This same advocate asserted that the President appointed "the strongest, most qualified team in history to protect government and corporate whistleblowers."[15]

a. Merit Systems Protection Board

For example, in 2009, Obama appointed Susan Tsui Grundmann as Chairman of the Merit Systems Protection Board (MSPB) and Anne Marie Wagner as Vice Chairman. The MSPB hears appeals from administrative judges of complaints by federal employees, including whistleblowers, re-

12. SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 177 (1982).

13. Whistleblower advocacy groups greeted these nominations with acclaim, likely indicating the extent to which these appointments support whistleblowers generally. *See, e.g.*, Press Release, Gov't Accountability Project, GAP Executive Director to Become Deputy Special Counsel (June 15, 2011), *available at* <http://www.whistleblower.org/press/press-release-archive/1195-gap-executive-director-to-become-deputy-special-counsel> ("The Obama Administration has appointed a very strong team to lead the agencies that implement whistleblower laws.").

14. Chuchmach & Schwartz, *supra* note 1 (quoting Tom Devine of GAP).

15. *See* Tom Devine, *GAP Praises Confirmation of New Special Counsel Lerner*, GOV'T ACCOUNTABILITY PROJECT (Apr. 15, 2011), <http://www.whistleblower.org/blog/31-2010/1068-gap-praises-confirmation-of-new-special-counsel-lerner>.

lated to the Civil Service Reform Act of 1978 (CSRA) and the amendments to that act in the Whistleblower Protection Act of 1989 (WPA).[16] Grundmann was the general counsel for the National Federation of Federal Employees, and Wagner had been the general counsel for the Personal Appeals Board of the U.S. Government Accountability Office.[17] These appointments in particular signaled hope for whistleblowers because the MSPB under President Bush's nominees routinely ruled against whistleblowers: by one count the Bush MSPB found for a whistleblower in only one out of forty-five cases.[18]

Although it may still be early to completely assess the effect of these nominations, some moves by the new MSPB indicate a reversal of the old Board's harsh stance towards whistleblowers. By January 2011, one year into the new Board's tenure, whistleblowers had won half (four of eight) of the cases brought to the full MSPB.[19] One of the most visible of those cases, involving Washington D.C. Park Police Chief Theresa Chambers, highlights the Board's new approach under Obama's nominees. The Department of Interior had fired Chambers for disclosing that cutbacks in the Park Police budget resulted in increased public safety problems.[20] After previous Boards and the Federal Circuit earlier rejected Chambers' claims, the Obama MSPB overturned these decisions, restored her to her previous position, and awarded her backpay.[21] In another early case under the new Board, the MSPB found that the WPA protected whistleblower disclosures even if the disclosures violated an agency policy of confidentiality.[22] Also,

16. *See About MSPB*, U.S. MERIT SYS. PROTECTION BD., <http://mspb.gov/About/about.htm> (last visited Apr. 16, 2012). The CSRA, as amended by the WPA, provides retaliation protection to certain federal employees who report specific types of misconduct within the executive branches of the federal government.

17. Chuchmach & Schwartz, *supra* note 1.

18. *Id*. ("Unlike Bush Administration appointees who compiled a 1-44 track record against whistleblowers, these leaders are seasoned veterans with a proven track record of commitment to the merit system throughout their careers." (quoting Tom Devine from GAP)). The MSPB's miserable track record for whistleblowers actually goes further back than President G.W. Bush; Tom Devine testified to Congress that in 2,000 cases between 1979 and 1988, the Board ruled for whistleblowers four times on the merits. *See Protecting the Public from Waste, Fraud and Abuse: Hearing on H.R. 1507, The Whistleblower Protection Enhancement Act of 2009 Before the H. Comm. on Oversight & Gov't Reform*, 111th Cong. 11 (2009) (statement of Thomas Devine, Government Accountability Project) [hereinafter Devine Statement], *available at* <http://democrats.oversight.house.gov/images/stories/documents/20090513183928.pdf>. Since 2000, whistleblowers have won three out of 56 cases. *See id*.

19. Tom Devine, *MSPB Turnaround Highlights Problems with Administrative Judge System*, GOV'T ACCOUNTABILITY PROJECT (Feb. 1, 2011), <http://www.whistleblower.org/blog/31-2010/971-mspb-turnaround-highlights-problems-with-administrative-judge-system>. Tom Devine stated that "[f]or whistleblowers, to date the [new] Board's leadership has been turning on the lights after the Dark Ages." *Id*.

20. *See* Chambers v. Dep't of Interior, 2011 M.S.P.B. 7 ¶¶ 3-6 (2011).

21. *See id*. ¶¶ 49-50.

22. *See* Parikh v. Dep't of Veterans Affairs, 2011 M.S.P.B. 1 ¶¶ 18-19 (2011).

in 2011, the Board issued favorable rulings for whistleblowers, or vacated and remanded administrative judge decisions against whistleblowers, in at least seven cases – an extraordinary number given its previous record.[23]

In addition to issuing favorable rulings, Obama's MSPB appointees also signaled their understanding that whistleblower protection remains an important aspect of the Board's responsibility. For example, in December 2010, the Board released a detailed report on the status of federal employee whistleblower protections and the "difficulties" a whistleblower must overcome to receive protection.[24] Although the Board carefully did not take a position on whether the law should be changed,[25] the Board paved the way for legislative reform by highlighting the deficiencies in the current legal regime.[26] The Board also surveyed federal employees generally on their perceptions of various prohibited personnel practices, including whistleblowing,[27] and, most recently, released the results of a study examining whistleblowing in more detail, including how to encourage more employees to report misconduct.[28] At a minimum, then, the Obama MSPB appointees have taken their call to protect whistleblowers seriously and indicated that whistleblowers might actually have success through the administrative process set up by the CSRA and the WPA – propositions that many whis-

23. *See* King v. Dep't of Army, 2011 M.S.P.B. 83 ¶¶ 5-7 (2011) (finding that the WPA protects employees whose agencies *perceive* them to be whistleblowers, even if the employee never actually blew the whistle; and finding that the ALJ should have told the employee about the possibility of making a claim as a perceived whistleblower); Ingram v. Dep't of Army, 2011 M.S.P.B. 71 ¶¶ 4-6 (2011) (finding that employee had engaged in protected conduct when he objected to a department event the employee claimed would have violated ethical regulations and potentially reveal trade secrets of agency contractors); Usharauli v. Dep't Health & Human Servs., 2011 M.S.P.B. 54 ¶¶ 6-8 (2011) (finding that refusing to reappoint an employee and placing the employee on administrative leave are "personnel actions" under 5 U.S.C. § 2302(a)(2)(A) (2006) that could form the basis for a retaliation claim); Vaughn v. Dep't of Agriculture, 2011 M.S.P.B. 48 ¶¶ 5-7 (2011) (overturning an ALJ and finding that an agency had not fully complied with the Board's previous order in favor of a whistleblower); Peterson v. Dep't of Veterans Affairs, 2011 M.S.P.B. 38 ¶¶ 3-11 (2011) (finding that an ALJ improperly dismissed a whistleblower's claim at the pleading stage); Mason v. Dep't Homeland Sec., 2011 M.S.P.B. 39 ¶¶ 8-12 (2011) (vacating and remanding whistleblower case because the ALJ should have concluded that an employee engaged in protected conduct); Hamilton v. Dep't of Veterans Affairs, 2011 M.S.P.B. 35 ¶¶ 14-15 (2011) (vacating and remanding case because ALJ should have found that whistleblowing played a contributing factor in the employee's removal).

24. MERIT SYS. PROTECTION BD., WHISTLEBLOWER PROTECTIONS FOR FEDERAL EMPLOYEES, at unnumbered 2 (2010), *available at* <http://www.mspb.gov/netsearch/viewdocs.aspx?docnumber=557972 % 20&version=559604&application=ACROBAT>.

25. *See id*. at 2.

26. *See id*. at unnumbered 2 ("This report spells out in greater depth the difficulties a potential whistleblower may face when navigating the law to seek protection from agency retaliation.").

27. *See generally* MERIT SYS. PROTECTION BD., PROHIBITED PERSONNEL PRACTICES: EMPLOYEE PERCEPTIONS 32-33 (2011), *available at* <http://www.mspb.gov/netsearch/viewdocs.aspx?docnumber=634680&version=636592&application=ACROBAT>.

28. *See generally* MERIT SYS. PROTECTION BD., BLOWING THE WHISTLE: BARRIERS TO FEDERAL EMPLOYEES MAKING DISCLOSURES (2011), *available at* <http://www.mspb.gov/netsearch/viewdocs.aspx?docnumber=662503&version=664475&application=ACROBAT>.

tleblowers would have found hard to believe during previous administrations.[29]

b. Office of Special Counsel

Obama's appointments to the Office of Special Counsel (OSC) provide more examples. The OSC exists to protect federal government whistleblowers and to investigate their disclosures.[30] During the Bush presidency, the OSC did little to fulfill these roles, leading some whistleblower advocates to call it "dysfunctional."[31] OSC employees filed a formal complaint against Bush's Special Counsel, Scott Bloch, for issuing a gag order prohibiting employees from talking to anyone outside OSC about sensitive internal matters without prior clearance – an order that likely violated the First Amendment and federal law permitting employees to give information to Congress.[32] He also summarily dismissed hundreds of whistleblower cases in order to clear a backlog of pending matters.[33] Adding insult to injury, Bloch later resigned in disgrace amid charges that he had retaliated against whistleblowers in his own office.[34]

In June 2011, after leaving the Special Counsel position vacant for several years, Obama appointed as Special Counsel Carolyn Lerner, an experienced plaintiff's civil rights lawyer.[35] Lerner subsequently appointed Mark Cohen, the Executive Director of the Government Accountability Project (GAP), a whistleblower advocacy group, to become Deputy Special Counsel. The GAP President announced that "[t]his is a time of celebration for whistleblowers everywhere. . . . [Cohen] is exactly the kind of whistle-

29. This is not to say that the administrative process for federal whistleblowers works well. Tom Devine has argued that even though the MSPB has become more open to whistleblower complaints, the ALJs who adjudicate an employee's initial hearing remain hostile to whistleblowers. *See* Devine, *supra* note 19.

30. *See Introduction to OSC*, U.S. OFFICE OF SPECIAL COUNSEL, <http://www.osc.gov/Intro.htm> (last visited Apr. 16, 2012).

31. PROJECT ON GOV'T OVERSIGHT, HOMELAND AND NATIONAL SECURITY WHISTLEBLOWER PROTECTIONS: THE UNFINISHED AGENDA 13 (2005); *see also* Joe Davidson, *Federal Diary: Whistleblowers Get a Defender*, WASH. POST, Oct. 18, 2011, at B4 ("OSC is an independent federal agency with a long and well-deserved reputation for failing to protect federal whistleblowers.").

32. *See* Peter Katel, *Protecting Whistleblowers*, 16 CQ RESEARCHER 265, 278 (2006).

33. *See* PROJECT ON GOV'T OVERSIGHT, *supra* note 31, at 13-14.

34. *See* Joe Davidson, *Workers Applaud Special Counsel's Return to Private Sector*, WASH. POST, Oct. 22, 2008, at B4; Robert Brodsky, *White House Forces OSC Chief Out*, GOVEXEC.COM (Oct. 23, 2008), <http://www.govexec.com/oversight/2008/10/white-house-forces-osc-chief-out/27911/> (last visited Apr. 16, 2012). Bloch pled guilty to contempt of Congress after he had his computer hard drive erased when Congress began to investigate those allegations. Davidson, *supra* note 31. Subsequently, he successfully withdrew his guilty plea because he claimed he was not fully informed that his conviction would result in a mandatory jail sentence. *Id*.

35. *See Carolyn Lerner*, U.S. OFFICE OF SPECIAL COUNSEL, <http://www.osc.gov/Lerner.htm> (last visited Apr. 16, 2012).

blower advocate who should be working in the Office of Special Counsel."[36]

Within months of their appointments, Lerner and Cohen immediately altered the direction of the OSC by asking the Merit Systems Protection Board to prevent federal agencies from taking adverse personnel actions against two alleged whistleblowers,[37] an action the MSPB granted less than a week later.[38] Lerner stated that the unprecedented actions "make clear that this agency will vigorously protect federal employees against retaliation when they blow the whistle."[39] The National Whistleblowers Center remarked that the move "marks the beginning of new assertiveness by the OSC, and new grounds for optimism by federal employees at every level."[40] Indeed, the Department of Defense ultimately reinstated the security clearance of one whistleblower, allowing him to return to work.[41] This whistleblower, Franz Gayl, who reported the Marines for failing to provide protective armor for vehicles in Iraq, stated:

> The Office of Special Counsel (OSC) has been transformed under the inspiring leadership of Carolyn Lerner. Since her arrival in the summer of 2011 OSC has truly come to fulfill its intended mission as a Federal guardian of whistleblower rights. For example, OSC's determination to request a stay of an indefinite salary cutoff that would have starved me out of the Marines and the Merit Service Protection Board's willingness to support it, was the turning point in my case during the darkest hours this fall, when I thought it would be necessary to sell my home and give up. I don't think it was a coincidence that the Department of the Navy then issued a favorable security adjudication that now permits me to get back to work.[42]

Moreover, the OSC filed an amicus brief in the case of a prominent

36. Press Release, Gov't Accountability Project, GAP Executive Director to Become Deputy Special Counsel (June 15, 2011), *available at* <http://www.whistleblower.org/press/press-release-archive/2011/1195-gap-executive-director-to-become-deputy-special-counsel>.

37. Press Release, Office of Special Counsel, OSC Seeks Quick Action to Protect Two Public Health and Safety Whistleblowers (Oct. 8, 2011), *available at <www.osc.gov/documents/press/2011/pr11_17du.pdf>*.

38. *See* Special Counsel ex. rel. Hardy v. Dep't of Health & Human Servs., No. CB-1208-12-0002-U-1 (MSPB Oct. 14, 2011); Special Counsel ex. rel. Gayl v. Dep't of Navy, No. CB-1208-12-0001-U-1 (MSPB Oct. 13, 2011).

39. Press Release, Office of Special Counsel, *supra* note 37, at 2.

40. Nick Schwellenbach, Special Counsel Seeks Protection for Two Whistleblowers (Oct. 10, 2011), <http://pogoblo.typepad.com/pogo/2011/10/special-counsel-seeks-protection-for-two-whistleblowers.html> (quoting Richard Renner).

41. *See* Press Release, Govt. Accountability Project, MRAP Whistleblower to Return to Work (Nov. 16, 2011), <http://www.whistleblower.org/press/press-release-archive/1592-mrap-whistleblower-to-return-to-work>.

42. Marcus Baram, *Let's Ensure Whistleblowers' Good Deeds Go Unpunished*, THE HUFFINGTON POST (Nov. 21, 2011, 11:40 AM), <http://www.huffingtonpost.com/marcus-baram/making-sure-that-whistleb_b_1105272.html>.

whistleblower and former air marshal in his appeal of a MSPB administrative judge's ruling against him, arguing that the MSPB was improperly expanding a narrow exception to the Civil Service Reform Act.[43] Noting these moves, a long-time employment lawyer in Washington, D.C. stated that, "[b]y taking the position that [Lerner] did, and making it clear she was not going to be a wallflower or someone who could just be walked over, . . . she sent a very strong message that whistle-blowers would be protected."[44] According to the *Washington Post*, Lerner has brought a jolt of energy to the Office of Special Counsel because she took on long-neglected cases and, in several high-profile cases, has "gone to the mat and tried to expand the boundaries of the law's protections for whistleblowers."[45]

c. Administrative Review Board

One final area deserves mention: the Administrative Review Board (ARB) of the Department of Labor. The ARB hears the final administrative appeals of whistleblower claims under twenty-one different federal whistleblower laws.[46] As with his other appointments, Obama dramatically influenced the direction of the ARB. Obama's Secretary of Labor, Hilda Solis, appointed five new members to the ARB's five-member panel in 2010 and 2011, and, as two whistleblower advocates remarked, "[t]ogether they have the most experience, subject matter expertise, and demonstrated commitments to the board's mission of any members in its history."[47] For example, the Board's Chair, Paul Igasaki, formerly chaired the Equal Employment Opportunity Commission during President Bill Clinton's Administration and has worked for numerous non-profit civil rights organizations.[48] The Vice Chair, E. Cooper Brown, previously served on the ARB during Clinton's presidency, and another member, Joanne Royce, worked for GAP, the whistleblower advocacy group mentioned above, for fifteen

43. Stephen Losey, *Decision to Fire Air Marshal Risks Silencing Whistle-Blowers, OSC Says*, FEDERAL TIMES (last updated Aug. 26, 2011), <http://www.federaltimes.com/article/20110826/DEPARTMENTS03/108260301/>.

44. Carrie Johnson, *Government Whistle-Blowers Gain New Advocate*, NPR (Nov. 22, 2011), http://www.npr.org/2011/11/22/142599974/government-whistle-blowers-gain-new-advocate; see *also id*. ("The agency has switched from being poison ivy for whistle-blowers to being the first option for organizations like ours that are always looking for the best way to defend people who commit the truth.") (quoting Tom Devine).

45. Lisa Rein, *Special Counsel Carolyn Lerner Quickly Raises the Profile of Her Office*, WASH. POST, Dec. 25, 2011, at C1.

46. *See ARB – Areas of Responsibility*, U.S. DEP'T OF LABOR, <http://www.dol.gov/arb/areas.htm> (last visited Apr. 16, 2012); *The Whistleblower Protection Program*, U.S. DEP'T OF LABOR, <http://www.whistleblowers.gov/index.html> (last visited Apr. 16, 2012).

47. DEVINE & MAASSARANI, *supra* note 1, at 183.

48. *ARB Board Members*, U.S. DEP'T. OF LABOR, <http://www.dol.gov/arb/members.htm> (last visited Apr. 16, 2012).

years.[49]

During a six-month period in 2010 after the appointment of four of these new members, whistleblowers won six out of sixteen cases (37.5 percent) before the ARB on the merits, as opposed to 19.75 percent (eight out of forty-one cases) in 2009.[50] However, more than just statistics indicate the sea change caused by their appointments. The ARB's recent decisions, particularly with regard to the Sarbanes-Oxley Act of 2002, expanded the scope of whistleblower protections and overturned numerous Bush-era decisions adverse to whistleblowers. For example, when President Bush's appointees dominated the Board, the ARB had a narrow view of the scope of protected conduct under Sarbanes-Oxley. Although the Act's terms protected employees who reported any of six different types of misconduct,[51] including violations of broad statutory provisions prohibiting mail and wire fraud, the Bush ARB held that any whistleblower report must *also* "be of a type that would be adverse to investors' interests."[52] If a whistleblower reported what she reasonably believed to be securities fraud, then the ARB also required that the whistleblower demonstrate the fraud was material, which in essence required proving *actual* securities fraud, not just that the whistleblower "reasonably believed" securities fraud occurred as required by the statute's plain language.[53] Moreover, the ARB held that a whistleblower's protected disclosure must "'definitively and specifically' relate to any of the listed categories of fraud or securities violations"[54] – another requirement absent from the statutory language.

In the summer of 2011, the new ARB overturned those holdings in several sweeping opinions. First, the Board found that allegations of mail and wire fraud did *not* also need to relate to shareholders' interests.[55] Se-

49. *Id*.

50. DEVINE & MAASSARANI, *supra* note 1, at 183.

51. *See* 18 U.S.C. § 1514A (2006) (prohibiting retaliation against an employee who reports conduct the employee reasonably believes violates laws against mail fraud, wire fraud, banking fraud, securities fraud, "any rule or regulation of the Securities and Exchange Commission, or any provision of Federal law relating to fraud against shareholders").

52. *See* Platone v. FLYi, Inc., ARB Case No. 04-154, at 15 (Sept. 20, 2006), *available at* <http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARB_DECISIONS/SOX/04_154.SOXP.PDF>.

53. *See id*. at 16.

54. *See id*. at 17 (quoting Kester v. Carolina Power & Light Co., ARB No. 02-007, ALJ No. 2000-ERA-31, slip op. at 9 (Sept. 30, 2003), and adopting that case's interpretation of the whistleblower provision of a different statute, the Energy Reorganization Act (ERA) of 1974, 42 U.S.C. § 5851 (2006)).

55. *See* Brown v. Lockheed Martin Corp., ARB Case No. 10-050, at 9 (Feb. 28, 2011), *available at* <http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARB_DECISIONS/SOX/10_050.SOXP.PDF>; see also Funke v. Federal Express Corp., ARB Case No. 09-004, at 8 (July 8, 2011), *available at* <http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARBDECISIONS/SOX/09004.SOXP.PDF>; Sylvester v. Parexel, Int'l, ARB Case No. 07-123, at 21 (May 25, 2011), *available at* <http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARB_DECISIONS/SOX/07_123.SOXP.PDF>. The Board arguably went even further and found that a whistleblower's protected disclosure did not have to disclose

cond, the Board rejected its earlier holding regarding "materiality," by finding that a whistleblower will be protected when disclosing fraudulent conduct, even if a reasonable shareholder would not consider it important in deciding how to vote.[56] Third, the Board criticized the use of the "definitively and specifically" standard as "inappropriate" because it was imported from a case interpreting a different whistleblower statute with language not found in Sarbanes-Oxley.[57]

Other cases reflected the ARB's willingness to apply the Act's protections broadly. For example, almost immediately after Congress passed Sarbanes-Oxley in 2002, the issue arose whether privately-held subsidiaries of publicly-traded companies could be held liable under Sarbanes-Oxley's antiretaliation provision.[58] The Bush ARB had determined that Sarbanes-Oxley could cover a subsidiary, but only when the subsidiary acted as an agent for a publicly-traded parent specifically to retaliate against the employee – a relatively narrow interpretation.[59] After this decision, administrative law judges (ALJs) and courts still debated the issue until 2010,[60] when Congress passed the Dodd-Frank Wall Street Reform and Consumer Protection Act.[61] Dodd-Frank amended Sarbanes-Oxley to make clear that the Act prohibited subsidiaries of publicly-traded companies from retaliating against whistleblowers.[62] Although this legislation resolved the issue going forward, the question remained whether the inclusion of subsidiaries in Sarbanes-Oxley would apply retroactively for cases that arose before

fraudulent conduct at all, as long as it could be seen as "in furtherance of a scheme or artifice to defraud." *Brown*, ARB Case No. 10-050, at 9.

56. *Sylvester*, ARB Case No. 07-123, at 21. The Board did leave open the possibility that a complaint may concern "such a trivial matter" that there is no protected activity. *See id*. at 22.

57. *Id*. at 18.

58. *See* Richard E. Moberly, *Unfulfilled Expectations: An Empirical Analysis of Why Sarbanes-Oxley Whistleblowers Rarely Win*, 49 WM. & MARY L. REV. 65, 110-13, 134-37 (2007).

59. *See* Klopfenstein v. PCC Flow Tech. Holdings, Inc., ARB No. 04-149, at 15 (May 31, 2006), *available at* <http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARB_DECISIONS/SOX/04_149.SOXP.PDF>. This restriction arguably contravened the purpose of the statute and resulted in numerous dismissals of whistleblower cases by Department of Labor Administrative Law Judges. *See* Moberly, *supra* note 58, at 134-37.

60. *See* Johnson v. Siemens Bldg. Techs., Inc., ARB No. 08-032, at 10-11 (Mar. 31, 2011), *available at* <http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARB_DECISIONS/SOX/08_032A.SOXP.PDF> (citing cases with different holdings regarding this issue).

61. Pub. L. No. 111-203, 124 Stat. 1376 (2010) [hereinafter Dodd-Frank Act] (codified at scattered sections of the U.S. Code).

62. Section 929A of the Dodd-Frank Act amended Sarbanes-Oxley section 806(a) to add the following italicized language regarding the entities that may not retaliate against a whistleblower: "No company with a class of securities registered under section 12 of the Securities Exchange Act of 1934 (15 U.S.C. 781), or that is required to file reports under section 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 780(d)), . . . *including any subsidiary or affiliate whose financial information is included in the consolidated financial statements of such company*, [may retaliate]." Pub. L. No. 111-203, § 929A, 124 Stat. at 1852 (codified at 18 U.S.C. § 1514A(a) (Supp. IV 2010)).

Dodd-Frank's enactment. The new Obama ARB determined that Dodd-Frank merely clarified Sarbanes-Oxley's true meaning, and that Sarbanes-Oxley should have always included subsidiaries as covered entities, essentially overturning Bush-era precedent.[63]

The new ARB also interpreted Sarbanes-Oxley broadly to expand the concept of who could receive whistleblower reports. Sarbanes-Oxley's language states that, in order to receive protection, a whistleblower must report misconduct to "(A) a Federal regulatory or law enforcement agency; (B) any Member or committee of Congress; or (C) a person with supervisory authority over the employee (or such other person working for the employer who has the authority to investigate, discover, or terminate misconduct)."[64] In July 2011, the ARB interpreted this language to include a report to local or state law enforcement, despite the ambiguity in the statutory language regarding whether "Federal" in subsection A modifies "law enforcement agency" as well as "regulatory."[65] Only protecting reports to federal law enforcement would, according to Obama's ARB, result in a "hypertechnical distinction" that would be inconsistent with the goal of the statute to promote disclosures.[66] In September 2011, the ARB also determined that Sarbanes-Oxley protected whistleblowers who reported to the IRS as part of its whistleblower bounty program, because the IRS is a "Federal regulatory . . . agency."[67]

Obama's ARB expanded upon what would be considered an "adverse action" under Sarbanes-Oxley. In *Menendez v. Halliburton*,[68] an employee had reported violations of accounting standards to the company and the SEC.[69] Although this whistleblowing qualified as protected activity, the ALJ held that the employee did not suffer any retaliatory adverse action.[70] The new ARB, however, reversed this decision and detailed an easy standard for plaintiffs to meet in order to satisfy the "adverse action" element of a Sarbanes-Oxley claim.[71] The ARB stated that "minor acts of retaliation can be sufficiently substantial when viewed together," and therefore held

63. *See Johnson*, ARB No. 08-032, at 16.

64. 18 U.S.C. § 1514A(a)(1).

65. *See* Funke v. Federal Express Corp., ARB Case No. 09-004, at 16 (July 8, 2011), *available at* <http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARB_DECISIONS/SOX/09_004.SOXP.PDF>.

66. *Id*.

67. *See* Vannoy v. Celanese Corp., ARB No. 09-118, at 12 (Sept. 28, 2011), *available at* <http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARB_DECISIONS/SOX/09_118.SOXP.PDF>.

68. ARB Nos. 09-002 & 09-003 (Sept. 13, 2011), *available at* <http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARB_DECISIONS/SOX/09_002.SOXP.PDF>.

69. *See id*. at 2-4.

70. *See id*. at 9, 11.

71. *See id*. at 21.

that a whistleblower could recover if retaliation was "more than trivial,"[72] a standard that likely would cover a broader range of retaliatory actions than the Supreme Court previously found actionable for Title VII claims in *Burlington Northern & Santa Fe Railway Co. v. White*.[73] The ARB in *Menendez* used this new standard to find an adverse action when a company merely released the name of the whistleblower to its employees as part of its internal investigation into the employee's complaint.[74]

In addition to broadening Sarbanes-Oxley's reach, the new ARB restricted employer defenses. In one remarkable case, Obama's ARB even seemed to undermine an employer's ability to fire an employee for revealing confidential information and taking confidential documents, if the employee uses that information and those documents as part of the whistleblowing process. In *Vannoy v. Celanese Corp.*,[75] a whistleblower took confidential employer documents, including information related to personal information of current and former employees, to help substantiate his claims of wrongdoing.[76] The ALJ agreed with the employer's argument that it fired the employee because he violated his confidentiality agreement with the company, and therefore the employee did not demonstrate that the employee's whistleblowing was a contributing factor in his dismissal and that, even if the firing and the whistleblowing were connected, the employer proved by clear and convincing evidence that it would have fired the employee anyway because of the breach of confidentiality.[77] However, the ARB determined that the ALJ did not give sufficient weight to the employee's need for internal documents in order to provide original information to government regulators, and the ARB remanded the case for a further evidentiary hearing, noting that, "[t]here is a clear tension between a company's legitimate business policies protecting confidential information and the whistleblower bounty programs created by Congress to encourage whistleblowers to disclose confidential company information in furtherance

72. *Id*.

73. 548 U.S. 53 (2006). The ARB distinguished *Burlington Northern* and found that the case was helpful in determining the scope of prohibited actions, but was not dispositive because Sarbanes-Oxley clearly prohibits "a very broad spectrum" of retaliatory activity, including non-tangible adverse actions. *See Menendez*, ARB Nos. 09-002 & 09-003, at 15-16.

74. *Menendez*, ARB Nos. 09-002 & 09-003, at 22-26. The ARB supported this conclusion by noting that this breach of confidentiality violated Sarbanes-Oxley Section 301's requirement that companies provide a confidential, anonymous reporting channel for whistleblowers to report misconduct. *See id*.

75. ARB No. 09-118 (Sept. 28, 2011), *available at* <http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARB_DECISIONS/SOX/09_118.SOXP.PDF>.

76. *Id*. at 5.

77. *Id*. at 7-8.

of enforcement of tax and securities laws."[78]

The ARB's new approach also can be seen in the way in which it is deciding cases. In the first few years of Sarbanes-Oxley cases, ALJs tended to dismiss cases based on summary adjudications, finding that whistleblowers failed to prove their cases as a matter of law.[79] In the few cases in which ALJs held hearings, whistleblowers fared much better, supporting the notion that whistleblower cases often present fact-intensive issues that need evidentiary hearings to explore.[80] The new ARB seems to be sending a message to ALJs that they should prefer evidentiary hearings over summary dispositions. In *Sylvester v. Parexel International, Inc.*,[81] the ARB stated that "Rule 12 motions challenging the sufficiency of the pleadings are highly disfavored by the SOX regulations and highly impractical under the Office of Administrative Law Judge (OALJ) rules,"[82] in part because they involve "inherently factual issues such as 'reasonable belief' and issues of 'motive'."[83] Also, in *Vannoy v. Celanese Corp.*,[84] the ARB reversed a summary disposition in favor of the employer and ordered the ALJ to conduct a detailed and specific evidentiary hearing.[85] It may be too early to tell whether these cases constitute a trend toward demanding that ALJs issue fewer summary judgments, but the ARB cases from 2011 seem, at a minimum, to indicate that the ARB understands the negative impact summary dispositions can have on whistleblowers.

2. Legislation

President Obama also demonstrated his belief in the importance of whistleblowing by supporting the addition of whistleblower protections in his most significant legislative achievements: the economic stimulus package, health care reform, and the reform of the financial industry.

a. Stimulus Bill

Immediately after taking office, President Obama signed the American Recovery and Reinvestment Act of 2009,[86] also called the "Stimulus Bill,"

78. *Id*. at 15-17.

79. *See* Moberly, *supra* note 58, at 104-05.

80. *See id*. at 127-28.

81. ARB No. 07-123 (May 25, 2011), *available at* <http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARB_DECISIONS/SOX/07_123.SOXP.PDF>.

82. *Id*. at 13.

83. *Id*.

84. ARB No. 09-118, at 12 (Sept. 28, 2011), *available at* <http://www.oalj.dol.gov/PUBLIC/ARB/DECISIONS/ARB_DECISIONS/SOX/09_118.SOXP.PDF>.

85. *Id*. at 14-17.

86. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 1553, 123 Stat. 115,

to respond to the recession and to create jobs. The Act protects a broad range of disclosures by employees of non-Federal employers that receive stimulus funds.[87] On paper, the Act's antiretaliation provision follows the "best practices" that began with Sarbanes-Oxley in 2002 and have developed in the last decade, including a burden of proof that seems favorable to whistleblowers.[88] Moreover, whistleblowers can report violations to a wide range of institutions and individuals, including both internal and external recipients.[89] The Act provides for an administrative remedy first, but, like Sarbanes-Oxley, permits whistleblowers to file claims in federal district court if the administrative process is not completed in a timely manner.[90]

Importantly, the Act's whistleblower provision also implements new innovations that would be repeated by other Obama whistleblower protections. It prohibits the use of pre-dispute arbitration provisions to force a whistleblower to arbitrate claims brought under the Act.[91] Additionally, the Act expressly permits whistleblowers to use circumstantial evidence to demonstrate that their protected activity played a "contributing factor" in the employer's retaliation, specifically including "evidence that the official undertaking the reprisal knew of the disclosure" or "evidence that the reprisal occurred within a period of time after the disclosure such that a reasonable person could conclude that the disclosure was a contributing factor

297 (codified in scattered sections of the U.S. Code).

87. *See id*. § 1553(a)(1)-(5), 123 Stat. 297 (protecting disclosures related to use of the stimulus funds, including a gross waste of the funds, gross mismanagement of them, or a violation of law related to use of the funds).

88. An employee must demonstrate that a protected disclosure was a "contributing factor" in an employer deciding to take an adverse employment action against the employee. *See id*. § 1553 (c)(1)(A)(i), 123 Stat. 299. If the employee succeeds, the employer will be held liable for damages resulting from the retaliation unless the employee can demonstrate by clear and convincing evidence that it would have taken the same action regardless of the protected activity. *See id*. § 1553(c)(1)(B), 123 Stat. 299.

89. *See id*. § 1553(a), 123 Stat. 297 (protecting disclosures made to "the [Recovery Accountability and Transparency] Board, an inspector general, the Comptroller General, a member of Congress, a State or Federal regulatory or law enforcement agency, a person with supervisory authority over the employee (or such other person working for the employer who has the authority to investigate, discover, or terminate misconduct), a court or grand jury, the head of a Federal agency or their representatives").

90. *See id*. § 1553(c)(3), 123 Stat. 300 (permitting a whistleblower to file a claim for a jury trial in federal court if the inspector general of the federal agency has not issued an order within 210 days after the submission of a complaint or has denied the whistleblower's claim). The whistleblower must first report retaliation to an appropriate inspector general, who must then investigate and submit a report to the whistleblower and the employer within 180 days. *See id*. § 1553(b), 123 Stat. 297-98.

91. *See id*. § 1553(d), 123 Stat. 301. The Dodd-Frank Wall Street Reform and Consumer Protection Act and the Patient Protection and Affordable Care Act of 2009 both have similar provisions. *See* The Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 1558(b)(2), 124 Stat. 119, 261 (2010) ("The rights and remedies in this section may not be waived by any agreement, policy, form, or condition of employment."); Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, § 748, 124 Stat. 1376, 1739 (2010); *id.* § 1057, 124 Stat. at 2031.

in the reprisal."[92]

b. Health Care Reform

Second, on March 23, 2010, Obama signed the Patient Protection and Affordable Care Act (PPACA),[93] commonly known as health care reform. The PPACA protects employees from retaliation if they report violations of the Act.[94] Although not as detailed as the Stimulus Bill's provision, the PPACA's whistleblower protections still provide the strong whistleblower protections found in other recent federal statutes, including permitting employees to make reports of misconduct internally or externally, and protecting employees who refuse to violate the Act.[95] The PPACA also adopts the employee-friendly burden of proof and procedures set out in recent whistleblower provisions such as Sarbanes-Oxley and the Consumer Product Safety Improvement Act.[96] In other words, the whistleblower must file an initial administrative claim with the Occupational Health and Safety Administration in the Department of Labor, which will determine whether the whistleblower's protected activity was a "contributing factor" in an adverse employment action.[97] If so, the whistleblower will prevail, unless the employer proves by clear and convincing evidence that it would have taken the same action regardless of the protected activity.[98] Moreover, if the Department of Labor does not finish its administrative review within 210 days, the whistleblower may file a *de novo* claim for a jury trial in federal district court.[99]

c. Wall Street Reform

Third, Obama signed the Dodd-Frank Wall Street Reform and Consumer Protection Act on July 21, 2010.[100] While his other major legislative achievements included antiretaliation provisions that mirrored other statutes, Dodd-Frank truly revolutionized whistleblower law in the United

92. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 1553(c)(1)(A)(ii)(I) & (II), 123 Stat. 115, 299.

93. The Patient Protection and Affordable Care Act, Pub. L. No. 111-148, 124 Stat. 119 (2010).

94. *Id*. § 1558(a), 124 Stat. 261.

95. *See id*.

96. *See id*. § 1558(b), 124 Stat. 261 (adopting procedures of Consumer Product Safety Improvement Act, 15 U.S.C. § 2087(b) (Supp. IV 2010)); *cf*. 49 U.S.C. § 42121(b) (2006) (whistleblower procedures adopted by Sarbanes-Oxley Act of 2002, 18 U.S.C. § 1514A(b) (2006)).

97. *See* 15 U.S.C. § 2087(b); 49 U.S.C. § 42121(b).

98. *See id.*

99. *See* 15 U.S.C. § 2087(b)(4) (adopted by The Patient Protection and Affordable Care Act, § 1558(b), 124 Stat. 261); *cf*. *id*. § 1514A(b)(1)(B) (permitting federal court claim after 180 days without a final resolution by the Department of Labor); 18 U.S.C. § 1514A(b)(2)(E) (permitting jury trial).

100. Pub. L. No. 111-203, 124 Stat. 1376 (2010).

States. Most importantly, the Act permits whistleblowers to file for rewards of 10 percent to 30 percent of any enforcement penalties recovered by the Securities and Exchange Commission and the Commodity Futures Trading Commission.[101] These provisions attempt to adopt the False Claims Act's "bounty" model, which has been utilized successfully for decades to reward whistleblowers who reported fraud on the government.[102] Dodd-Frank extends this concept to reports of securities and commodities fraud on the general public.[103]

Within a year after Dodd-Frank's passage, the Securities and Exchanges Commission (SEC) released rules and regulations implementing the Act's "bounty" program.[104] The three Democrats on the SEC, including Chairman Mary Schapiro, the one Commissioner able to be appointed by President Obama at the time, approved the controversial regulations over dissenting votes by the two Republicans appointed by President George W. Bush.[105] Despite heavy lobbying and pressure from business interests,[106] the SEC refused to require whistleblowers to report internally through a company's grievance procedure before reporting to the SEC (although the regulations do include incentives for internal reporting).[107] Moreover, the SEC changed its proposed definition of whistleblower from one who re-

101. *Id*. § 922(a), 124 Stat. 1841 (2010) (codified at 15 U.S.C. § 78u-6(b) (Supp. IV 2010)) (SEC); *Id.* § 748, 124 Stat. 1739 (2010) (codified at 7 U.S.C. § 26).

102. *See* Elletta Sangrey Callahan & Terry Morehead Dworkin, *Do Good and Get Rich: Financial Incentives for Whistleblowing and the False Claims Act*, 37 VILL. L. REV. 273, 278-82 (1992). Unlike the False Claims Act, however, Dodd-Frank does not permit the whistleblower to litigate claims on behalf of the government.

103. Pub. L. No. 111-203 § 922(a), 124 Stat. 1841 (codified at 15 U.S.C. § 78u-6(a)(6)) (defining "whistleblower" as "any individual who provides . . . information relating to a violation of the securities laws").

104. *See* Securities Exchange Act, Release No. 34-64545, File No. S7-33-10 (May 25, 2011) (to be codified at 17 CFR pts. 240 and 249). The Commodity Futures Trading Commission issued substantially similar regulations. *See* Final Rules for Implementing the Whistleblower Provisions of Section 23 of the Commodities Futures Act, 76 F.R. 53172 (Aug. 25, 2011). In this article, I will focus on the SEC provisions.

105. The five-year terms of the Commissioners are staggered so that one term ends on June 5 each year, and no more than three Commissioners may belong to the same political party. *See Current SEC Commissioners*, U.S. SEC. & EXCH. COMM'N, <http://sec.gov/about/commissioner.shtml> (last visited Apr. 17, 2012). President Obama inherited a Commission with two Democrats, Ellise Walter and Luis Aguilar, and he appointed another Democrat, Chairman Mary Schapiro. *SEC Historical Summary of Chairmen and Commissioners*, U.S. SEC. & EXCH. COMM'N, <http://sec.gov/about/sechistoricalsummary.htm> (last visited Apr. 17, 2012) (providing information about presidential appointments and political affiliation of commissioners). All three Democrats voted for the rules, while Commissioners Paredes and Casey, both Republicans appointed by President Bush, dissented. *See id*.; *Resources*, *Office of the Whistleblower*, U.S. SEC. & EXCH. COMM'N, <http://www.sec.gov/about/offices/owb/owb-resources.shtml#remarks> (last visited Apr. 17, 2012) (providing the Commissioners' remarks on the rules).

106. The SEC received 240 comment letters and approximately 1,300 form letters regarding the proposed rules. *See* Securities Whistleblower Incentives and Protections, 76 Fed. Reg. 34,300, 34,300 (June 13, 2011).

107. *See id*. at 34,324-27.

ports "potential" violations to one who reports a "possible" violation that may be "about to occur," and the whistleblower must simply have a "reasonable belief" that the violation might occur.[108] The new rules also provided some retaliation protection for auditors, lawyers, and other compliance personnel who report misconduct – a stark difference from the proposed rules that mostly denied protection to these whistleblowers.[109] Many perceived the SEC's rejection of industry demands as a positive sign that the SEC would begin to take whistleblowers seriously,[110] although this remains to be seen because the first awards will not be issued until sometime in 2012. However, within seven weeks of the beginning of the SEC's Dodd-Frank program, the SEC received 334 whistleblower tips,[111] the quality of which, according to a former SEC lawyer, has been "remarkably high."[112]

Additionally, Dodd-Frank included another strong antiretaliation provision that permits whistleblowers to bring claims for retaliation directly in federal district court.[113] In fact, the Act appears to provide corporate whistleblowers an interesting alternative to Sarbanes-Oxley: because Dodd-Frank's protected conduct includes making a disclosure protected by Sarbanes-Oxley,[114] whistleblowers who make disclosures protected by both statutes may opt to bring a Dodd-Frank claim because the statute of limitations is significantly longer (three years versus 180 days for Sarbanes-Oxley) and the Act permits two times the amount of back pay owed to the

108. *See id*. at 34,302-04.

109. *See id*. at 34,314-17.

110. *See* Thad Guyer, *Final Dodd-Frank Whistleblower Rules: Are You Prepared?*, GOV'T ACCOUNTABILITY PROJECT (June 15, 2011), <http://www.whistleblower.org/storage/documents/Guyer.pdf> (noting that SEC often chose whistleblower-friendly rules when faced with two choices); Richard Renner, *SEC's Dodd-Frank Rules Are a Major Victory for Whistleblowers*, WHISTLEBLOWERS PROT. BLOG (May 25, 2011), <http://www.whistleblowersblog.org/2011/05/articles/whistleblowers-tax-fraud/secs-doddfrank-rules-are-a-major-victory-for-whistleblowers/> ("The outcome [of the new rules] is a major victory for whistleblowers."); Press Release, Gov't Accountability Project, SEC Issues Win-Win Whistleblower Rules (May 26, 2011), *available at* <http://www.whistleblower.org/press/press-release-archive/1134-sec-issues-win-win-whistleblower-rules> ("Yesterday the SEC took the high road to strengthen the role of whistleblowers against corporate fraud. It rejected demands by a big business 'fraud lobby' and House Republicans to twist whistleblowing into obstruction of justice.").

111. *See* U.S. SEC. & EXCH. COMM'N, ANNUAL REPORT ON THE DODD-FRANK WHISTLEBLOWER PROGRAM, FISCAL YEAR 2011, at 5 (2011), *available at* <http://sec.gov/about/offices/owb/whistleblower-annual-report-2011.pdf>. The report covers claims from Aug. 12, 2011, the date the regulations became effective, until Sept. 30, 2011, the end of the fiscal year. *See id*.

112. *See* Samuel Rubenfeld, *SEC Receives 334 Tips in First Seven Weeks of Whistleblower Program*, WALL ST. J. (Nov. 16, 2011, 3:21 PM), <http://blogs.wsj.com/corruption-currents/2011/11/16/sec-receives-334-tips-in-first-seven-weeks-of-whistleblower-program/>.

113. *See* Dodd-Frank Act, Pub. L. No. 111-203, § 922(a), 124 Stat. 1376, 1841 (2010) (codified at 15 U.S.C. § 78u-6(h)(1)(B)(i) (Supp. IV 2010)).

114. *See id*. (codified at 15 U.S.C. § 78u-6(h)(1)(A)(iii)).

whistleblower, a bonus that Sarbanes-Oxley does not offer.[115] Furthermore, Dodd-Frank fixed some of the flaws that had become apparent in Sarbanes-Oxley's antiretaliation provision,[116] such as extending Sarbanes-Oxley's statute of limitations from ninety to 180 days, adding an explicit right to a jury trial if a whistleblower brings a claim in federal court, and clarifying that Sarbanes-Oxley protects employees of privately-held subsidiaries of publicly-traded companies.[117] It also provides new whistleblower protection for employees in the financial services industry who report fraud or illegal conduct related to the provision of a consumer financial product or service.[118]

d. Other Legislation

Other legislation passed during Obama's presidency contained whistleblower protections. The Fraud Enforcement and Recovery Act of 2009 (FERA)[119] closed loopholes in the False Claims Act to better encourage whistleblowers to report fraud on the government.[120] For example, FERA extended antiretaliation protection to contractors, sub-contractors, and agents who report fraud in addition to "employees" that the FCA already covered.[121] Also, the Coast Guard Authorization Act of 2010[122] amended the Seaman's Protection Act[123] to greatly expand the types of conduct in which a seaman can engage to be protected from retaliation[124] and to provide the same type of "best practices" burdens of proof, administrative remedies, and *de novo* review in federal district court as Sarbanes-Oxley

115. *Compare id*. (codified at 15 U.S.C. § 78u-6(h)(1)(B)(iii)(I)(bb)) (three year statute of limitations) *and id*. § 922(a) (codified at 15 U.S.C. § 78u-6(h)(1)(C)(ii)) (double back pay damages) *with* 18 U.S.C. § 1514A(b)(2)(D) (2006) (180 day statute of limitations) *and id*. § 1514A(c) (permitting damage claim for back pay, but not two times back pay).

116. *See generally* Moberly, *supra* note 58, at 132-37 (pointing out flaws in Sarbanes-Oxley's antiretaliation provision).

117. *See* Dodd-Frank Act, § 922(c), 124 Stat. 1848 (codified at 18 U.S.C. § 1514A(b)(2)(D)) (180 days); *id*. (codified at 18 U.S.C. § 1514A(b)(2)(E)) (jury trial); *id*., § 929A, 124 Stat. 1852 (codified at 18 U.S.C. § 1514A) (adding language regarding subsidiaries).

118. *See id.* § 1057, 124 Stat. 2031 (codified at 12 U.S.C. § 5567).

119. Pub. L. No. 111-21, 123 Stat. 1617 (2009) [hereinafter FERA].

120. The Senate Report accompanying the legislation noted that the changes were necessary because "[t]he effectiveness of the False Claims Act has recently been undermined by court decisions which limit the scope of the law and, in some cases, allow subcontractors paid with Government money to escape responsibility for proven frauds." S. REP. NO. 111-10, at 4 (2009). The Report also detailed the ways in which the FERA amended the FCA "to clarify and correct erroneous interpretations of the law" by the Supreme Court. *Id*. at 10.

121. FERA, § 4(d), 123 Stat. 1624 (codified at 31 U.S.C. § 3730(h)(1) (Supp. IV 2010)).

122. Pub. L. No. 111-281, § 611, 124 Stat. 2905, 2969 (2010).

123. 46 U.S.C. § 2114 (Supp. IV 2010).

124. Coast Guard Authorization Act § 611(a)(3), 124 Stat. 2969 (codified at 46 U.S.C. § 2114(a)(1)(C)-(G) (Supp. IV 2010)).

and the other recent antiretaliation statutes discussed above.[125] Most recently, the FDA Food Safety Modernization Act,[126] which President Obama signed on January 4, 2011, provided new whistleblower protections for employees who disclose violations of the Federal Food, Drug, and Cosmetic Act.[127] Once again, the Act utilized the same best practices from recent antiretaliation provisions.[128]

In many ways, then, President Obama fulfilled Candidate Obama's promises related to whistleblowing. His appointees arguably revolutionized whistleblower protection for both public and private employees. His legislative accomplishments included strong whistleblower protections. In short, whistleblower advocates have much to cheer after three years of an Obama Presidency. Yet, despite this strong support for whistleblowers generally, Obama seems to believe that one type of whistleblower should receive less robust protection: a whistleblower who makes disclosures related to national security, especially if one discloses classified information publicly, such as to the media.

B. National Security: The Great Exception

The "national security whistleblower," as I use the term here, either works for an agency in the "intelligence community,"[129] like the National

125. The Act deleted the previous provision allowing for a claim to be filed directly in federal court and adopted the "procedures, requirements, and rights" of the Surface Transportation Assistance Act (STAA), 49 U.S.C. § 31105(b) (Supp. IV 2010). *See* H.R. REP. NO. 111-303 § 2114 (2009) (showing deletions to old provision); Coast Guard Authorization Act § 611(a)(4), 124 Stat. 2969 (amending 46 U.S.C. § 2114(b) to reference 49 U.S.C. § 31105(b)). The STAA procedures, requirements, and rights mirror Sarbanes-Oxley's provisions. *Compare* 49 U.S.C. § 31105(b) *with* 18 U.S.C. § 1514A(b) (2006).

126. Pub. L. No. 111-353, 124 Stat. 3885 (2011).

127. *See id*. § 402, 124 Stat. 3968 (to be codified as 21 U.S.C. § 1012(a)).

128. *Compare id*. *with* 18 U.S.C. § 1514A(b) (2006).

129. The National Security Act of 1947, as amended, defines the "intelligence community" to include a wide variety of agencies:

(A) The Office of the Director of National Intelligence.

(B) The Central Intelligence Agency.

(C) The National Security Agency.

(D) The Defense Intelligence Agency.

(E) The National Geospatial-Intelligence Agency.

(F) The National Reconnaissance Office.

(G) Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs.

(H) The intelligence elements of the Army, the Navy, the Air Force, the Marine Corps, the Coast Guard, the Federal Bureau of Investigation, the Drug Enforcement Administration, and the Department of Energy.

(I) The Bureau of Intelligence and Research of the Department of State.

(J) The Office of Intelligence and Analysis of the Department of the Treasury.

(K) The elements of the Department of Homeland Security concerned with the analysis of intelligence information.

Security Agency, or reveals classified information (or both). As discussed below, in some cases the Obama Administration reacted with outright hostility to such whistleblowers, making a distinction between "bad" whistleblowing, which Obama calls "leaking" when it relates to national security, and "good" whistleblowing, which relates to non-security issues. In other instances, the Obama Administration reacted with more nuance by acknowledging the need for some protection for national security whistleblowers, but rejecting calls for the full panoply of rights the law typically provides other types of government whistleblowers.

1. Statements from Obama's Administration

The way the Obama Administration framed the issue through public statements demonstrates this more nuanced approach. For example, in March 2009, less than two months into his presidency, Obama gave some indication that he would make finer distinctions about whistleblowing than his statements as a candidate might indicate. He released a signing statement with a spending bill that provided protection to federal officials who reported information to Congress in which he stated that the bill should not be interpreted to undermine his authority to control communications with Congress "in cases where such communications would be unlawful or would reveal information that is properly privileged or otherwise confidential."[130] As the Brennan Center for Justice, a non-partisan public policy and law institute affiliated with New York University School of Law, noted,

> by objecting to a provision that was designed to prohibit retaliation against employees who reveal executive misconduct, President Obama's statement intentionally or unintentionally sends a message to employees: If you report misconduct to Congress against the will of the head of your agency, and if the agency considers that information "confidential," you may face retaliation. This could have a chilling effect on potential whistleblowers and hinder the public's ability to learn about government wrongdoing.[131]

Shortly thereafter, in November 2009, Robert S. Litt, who President

(L) Such other elements of any department or agency as may be designated by the President, or designated jointly by the Director of National Intelligence and the head of the department or agency concerned, as an element of the intelligence community.

50 U.S.C. § 401a(4) (2006).

130. Statement by the President (Mar. 11, 2009), *available at* <http://www.whitehouse.gov/the_press_office/Statement-from-the-President-on-the-signing-of-HR-1105>. The law prohibits the use of appropriations to pay salaries of anyone who "interferes with or prohibits" communications between federal employees and Congress related to the employee's job or agency. Omnibus Appropriations Act of 2009, Pub. L. No. 111-8, § 714(1), (2), 123 Stat. 524, 684.

131. *See* BRENNAN CTR. FOR JUSTICE AT N.Y. UNIV. SCH. OF LAW, TRANSPARENCY IN THE FIRST 100 DAYS: A REPORT CARD 23 (2009), *available at* <http://brennan.3cdn.net/07b3343e216944f6d9_ggm6ib3yb.pdf>.

Obama appointed as General Counsel for the Office of the Director of National Intelligence, promised action against "leaks of classified information that have caused specific and identifiable losses of intelligence capabilities."[132] More recently, in May 2011, Obama's appointment to head the Justice Department's national security division, Lisa Monaco, testified to Congress that "it would be my priority to continue the aggressive pursuit of [leak] investigations" because leaks do "tremendous damage."[133] Monaco noted that "twice as many" leak cases had been pursued during Obama's presidency than in all previous Administrations.[134] Similarly, after the raid that killed Osama bin Laden that same month, Leon Panetta, then the Director of the CIA, sent a memo to CIA employees stating, "Disclosure of classified information to anyone not cleared for it – reporters, friends, colleagues in the private sector or other agencies, former Agency officers – does tremendous damage to our work. At worst, leaks endanger lives."[135]

The media has corroborated that this anti-leak mentality begins at the top, asserting that Obama "is deeply troubled by leaks on sensitive national security matters like Afghanistan and Pakistan."[136] In his book, *The Promise*, Newsweek's Jonathan Alter wrote that "Obama had one pet peeve that could make him lose his cool . . . leaks."[137] Jane Mayer from *The New Yorker* related a conversation from a meeting between Obama and a group of advocates for more transparency in government, in which Obama "drew a sharp distinction between whistle-blowers who exclusively reveal wrongdoing and those who jeopardize national security."[138] Ms. Mayer described a statement of Danielle Brian from the Project on Government Oversight who attended the meeting, saying:

> Obama's tone was generally supportive of transparency. But when the subject of national-security leaks came up, Brian said, "the President shifted in his seat and leaned forward. He said this may be where we have some differences. He said he doesn't want to protect the people who leak to the media war plans that could impact the troops.[139]

132. Scott Shane, *Obama Steps up Prosecution of Leaks to the News Media*, N.Y. TIMES, June 12, 2010, at A1.

133. Shane, *supra* note 9.

134. *Id*.

135. *Leon Panetta Warns CIA Employees: No More OBL Raid Leaks*, ABC NEWS (May 19, 2011, 6:14 PM), <http://abcnews.go.com/blogs/politics/2011/05/leon-panetta-warns-cia-employees-no-more-obl-raid-leaks/>.

136. Gerstein, *supra* note 8.

137. JONATHAN ALTER, THE PROMISE 154 (2010). Alter reported that Obama is "fearsome" about leaks, although the leaks described in *The Promise* seem to relate to policy disputes that Obama believed were better handled internally rather than in the newspapers. *See id*. at 155.

138. *See* Mayer, *supra* note 7, at 48.

139. *See id*.

Unfortunately, as described in more detail below,[140] the line between whistleblowing and leaking may not be as clear as Obama asserted during that meeting. Nevertheless, the statement provides some context for evaluating President Obama's actions, which even more than his Administration's statements, demonstrate his approach to national security whistleblowers.

2. Actions by Obama's Administration

At the same time that it supported whistleblowers in the non-security context, Obama's Administration criminally prosecuted those who publicly disclosed conduct related to national security, conveyed a conspicuous lack of support for legislation that would improve protection for national security whistleblowers, and attempted to force reporters to reveal confidential sources for stories disclosing national security issues.

a. Criminal Prosecutions of Whistleblowers

Most alarmingly for whistleblower advocates, the Obama Administration used the Espionage Act, a statute typically reserved for the treasonous act of giving secret information to an enemy, to prosecute six individuals who could be described as whistleblowers because they gave information about misconduct to the media.[141] For example, the Obama (and Bush) Administrations criminally pursued Thomas Drake, a former employee of the National Security Agency (NSA), for allegedly disclosing classified information to a reporter.[142] Although Drake admitted telling a reporter that the NSA mismanaged certain projects and wasted almost $1 billion on a flawed surveillance system, he denied revealing any classified information.[143] Initially, prosecutors charged Drake with Espionage Act violations carrying a possible penalty of up to thirty-five years in jail.[144] However, the DOJ ultimately dropped almost all of the charges. After five years of investigation, Drake pled guilty to a misdemeanor charge of "exceeding authorized use of a computer" and did not receive any fine or jail time.[145]

The prosecution struck many observers as heavy-handed,[146] particular-

140. *See* discussion *infra* Part IV.A.

141. Savage, *supra* note 9; Shane, *supra* note 9. These prosecutions total more than the three previous cases brought by all previous Administrations combined. *See id*.

142. Mayer, *supra* note 7, at 47.

143. *See id*. at 55.

144. *Id*.; Glen Greenwald, *Obama's Whistleblower War Suffers Two Defeats*, SALON (July 30, 2011), <http://www.salon.com/news/department_of_justice/index.html?story=/opinion/greenwald/2011/07/30/whistleblowers>.

145. Ellen Nakashima, *Judge Blasts Prosecution of Alleged NSA Leaker*, WASH. POST, July 29, 2011, at A2.

146. *See generally* Mayer, *supra* note 7, at 48, 57 (describing reactions to prosecution). Even Ga-

ly when the Department of Defense Inspector General released a report substantiating Drake's claims about mismanagement and waste of public funds.[147] Moreover, the evidence that Drake possessed classified information was thin. Indeed, J. William Leonard, an official who was in charge of classifying information during the George W. Bush Administration, recently filed a complaint against the NSA for improperly classifying the document that formed the core of the government's case against Drake, stating that he had "never seen a more deliberate and willful example of government officials improperly classifying a document."[148] Remarkably, the judge even excoriated the prosecutors for their handling of the case, saying that the prosecution was "unconscionable" and did not "pass the smell test."[149]

Another example involves WikiLeaks, the website begun in 2007 to provide an anonymous place that whistleblowers from all over the world could post documents revealing government or corporate misconduct.[150] In 2010 and 2011, hundreds of thousands of classified U.S. government documents were provided to WikiLeaks, which posted them online and caused a diplomatic furor because they revealed embarrassing, and sometimes illegal, government conduct.[151] The Obama Administration reacted strongly: it added the organization to its list of enemies that threatened the security of the United States,[152] claimed that the release of documents put American troops in danger,[153] and ultimately arrested Army Private Bradley Manning for leaking many of the documents to the website.[154] Human rights activists

briel Schoenfeld, a noted conservative author who has argued for stronger protection of classified information, called the prosecution "draconian." *See id*. at 47.

147. *See* Kathleen McClellan, *Inspector General Report Vindicates GAP Clients From National Security Agency*, GOV'T ACCOUNTABILITY PROJECT (June 23, 2011), <http://www.whistleblower.org/blog/31/1207>; *see also* OFFICE OF THE INSPECTOR GEN. OF THE DEP'T OF DEF., REPORT 05-INTEL-03, REQUIREMENTS FOR THE TRAILBLAZER AND THINTHREAD SYSTEMS ii (2004), *available at* <*www.whistleblower.org/storage/documents/IGR.pdf*> ("[T]he NSA transformation effort may be developing a less capable long-term digital network exploitation solution that will take longer and cost significantly more to develop.").

148. *See* Scott Shane, *Complaint Seeks Punishment for Classification of Documents*, N.Y. TIMES, Aug. 2, 2011, at A16.

149. Nakashima, *supra* note 145.

150. *What is Wikileaks*, WIKILEAKS.ORG, <http://wikileaks.org/About.html> (last visited Apr. 17, 2012).

151. *See, e.g.*, Scott Shane, *Keeping Secrets WikiSafe*, N.Y. TIMES, Dec. 11, 2010, at WK1; Brad Knickerbocker, *WikiLeaks 101: Five Questions About Who Did What and When*, THE CHRISTIAN SCI. MONITOR, <http://www.csmonitor.com/USA/2010/1201/WikiLeaks-101-Five-questions-about-who-did-what-and-when/Who-is-responsible-for-the-leaks> (last visited Apr. 17, 2012).

152. *See* Stephanie Strom, *Pentagon Sees a Threat from Online Muckrakers*, N.Y. TIMES, Mar. 18, 2010, at A18.

153. *See* Scott Shane, *WikiLeaks Leaves Names of Diplomatic Sources in Cables*, N.Y. TIMES, Aug. 30, 2011, at A4.

154. *See* Kevin Poulsen & Kim Zetter, *U.S. Intelligence Analyst Arrested in Wikileaks Video*

criticized the Obama Administration for its treatment of Manning, who for the first year of his arrest reportedly was held in strict solitary confinement and made to sleep with a "suicide-proof smock" rather than his normal clothes.[155] The government also conducted a criminal grand jury investigation of WikiLeaks and its founder, Julian Assange,[156] that at least one source, the Australian embassy in Washington, D.C., reported to be "unprecedented both in its scale and nature."[157] Attorney General Eric Holder asserted publicly that publishing the government documents was a crime that should be prosecuted.[158] At the time of this writing, the outcome of that investigation has not been released publicly.[159]

Obama's DOJ prosecuted at least four other individuals for whistleblowing-type activities involving providing classified information to the media. In 2010, the DOJ prosecuted Shamai Leibowitz, a former FBI translator, for sending classified information to a blogger.[160] Leibowitz pled guilty to disclosing the transcripts from conversations overheard by an FBI wiretap at the Israeli Embassy in Washington DC, claiming that he was publicizing what he considered to be "a violation of the law."[161] The blogger who published the information agreed, stating that Leibowitz provided the transcripts to him "because of concerns about Israel's aggressive efforts to influence Congress and public opinion, and fears that Israel might strike nuclear facilities in Iran, a move he saw as potentially disastrous."[162]

Probe, WIRED.COM (June 6, 2010), <http://www.wired.com/threatlevel/2010/06/leak/>.

155. The Assoc. Press, *Germany: An Appeal to Obama Over a U.S. Prisoner's Treatment*, N.Y. TIMES, Apr. 14, 2011, at A13; *see also* Elisabeth Bumiller, *Pentagon to Move Suspect in Leaks*, N.Y. TIMES, Apr. 20, 2011, at A12 (noting that Amnesty International had concerns over Manning's treatment); Mark Benjamin, *WikiLeakers and Whistle-Blowers: Obama's Hard Line*, TIME (Mar. 11, 2011), <http://www.time.com/time/nation/article/0,8599,2058340,00.html>. Philip J. Crowley, a State Department spokesman stated that the Pentagon's treatment of Manning was "ridiculous, counterproductive and stupid," a comment leading to Crowley's subsequent resignation. *See* Bumiller, *supra*.

156. *See* Ellen Nakashima & Jerry Markon, *WikiLeaks Founder Could Face Charges*, WASH. POST, Nov. 30, 2010, at A1; Shane, *supra* note 9.

157. Philip Dorling, *US Targets WikiLeaks Like No Other Organisation*, SYDNEY MORNING HERALD, Dec. 3, 2011, at 10, *available at* <http://www.smh.com.au/technology/technology-news/us-targets-wikileaks-like-no-other-organisation-20111202-1obeo.html#ixzz1fVzUpHIT>.

158. *See* Julian E. Barnes & Evan Perez, *Assange Probe Hits Snag*, WALL ST. J., Feb. 9, 2011, at A3; *Assange Making Arrangements to Meet Police, Lawyer Says*, CNN (Dec. 6, 2010, 1:59 PM EST), <http://www.cnn.com/2010/US/12/06/wikileaks.investigation/index.html>.

159. In November 2011, a federal judge permitted the DOJ to subpoena information about WikiLeaks-related Twitter accounts. *See* Declan McCullagh, *Second Judge Gives DOJ Access to WikiLeaks-related Twitter Accounts*, CNET (Nov. 10, 2011, 12:24 PM PST), <http://news.cnet.com/8301-31921_3-57322538-281/second-judge-gives-doj-access-to-wikileaks-related-twitter-accounts/>.

160. Scott Shane, *Leak Offers Look at Efforts by U.S. to Spy on Israel*, N.Y. TIMES, Sept. 6, 2011, at A1.

161. Gerstein, *supra* note 8.

162. Shane, *supra* note 160; *see also* Richard Silverstein, *Why I Published US Intelligence Secrets About Israel's Anti-Iran Campaign*, TRUTHOUT (Oct. 14, 2011), <http://www.truth-out.org/why-i-published-us-intelligence-secrets-about-israels-anti-iran-campaign/1316550301>.

Leibowitz received a twenty-month prison sentence.[163]

Also in 2010, the Obama Administration charged Stephen J. Kim with violating the Espionage Act for allegedly providing classified information about North Korea to Fox News.[164] Kim is an expert on North Korea's nuclear program who consulted with the State Department and talked with Fox about how North Korea might respond to proposed U.S. sanctions.[165] In January 2011, the DOJ arrested former CIA officer Jeffrey Sterling and charged him with giving information to *New York Times* reporter James Risen about "a classified clandestine operational program designed to conduct intelligence activities" and a "human asset" Sterling had handled for the agency.[166] Finally, in January 2012, the DOJ charged former C.I.A. agent John Kiriakou with violating the Espionage Act by allegedly disclosing the identity of a C.I.A. analyst to a journalist.[167] The Government Accountability Project asserted that the government targeted Kiriakou because he had made public remarks questioning the use of waterboarding as an interrogation matter.[168]

Obama's predecessors used Espionage Act prosecutions far more sparingly. Before Obama became President, the government charged only three individuals with violating the Espionage Act for giving information to non-government actors, such as the media. The most famous of these cases involved Daniel Ellsberg and the Pentagon Papers in 1971, in which Ellsberg provided defense-related classified reports to the *New York Times*.[169] The case against Ellsberg was dismissed because of the prosecutors' ethical violations.[170] Previous to Leibowitz, the only successful Espionage Act prosecution of a government employee for giving classified information to a journalist occurred in 1984 when Samuel L. Morison was convicted of violating the Espionage Act by giving satellite photographs of a Soviet ship

163. Adam C. Estes, *Obama and Whistleblowers: Leak for Me but Not for Thee*, THE ATLANTIC WIRE (May 26, 2011), <http://www.theatlanticwire.com/business/2011/05/obama-whistleblowers-war-dodd-frank/38192/>.

164. Shane, *supra* note 9; Benjamin, *supra* note 155.

165. *See* Horton, *supra* note 8.

166. Pierre Thomas et al., *Ex-CIA Agent Jeffrey Sterling Arrested, Accused of Leaking to Reporter as Revenge*, ABC NEWS (Jan. 6, 2011), <http://abcnews.go.com/US/Blotter/cia-agent-jeffrey-sterling-arrested-accused-leaking-reporter/story?id=12557291>.

167. Savage, *supra* note 9.

168. Eric Tucker, Ex-CIA Officer charged with leaking secret info, *available at* <http://www.salon.com/2012/04/06/ex_cia_officer_charged_with_leaking_secret_info/> (last visited June 22, 2012).

169. N.Y. Times Co. v. United States, 403 U.S. 713, 714 (1971) (per curiam).

170. *See* Heidi Kitrosser, *Classified Information Leaks and Free Speech*, 2008 U. ILL. L. REV. 881, 899 n.115; William E. Lee, *Deep Background: Journalists, Sources, and the Perils of Leaking*, 57 AM. U. L. REV. 1453, 1477-78 (2008).

to *Jane's Defense Weekly*, a British publication.[171] Finally, in 2005, Lawrence Franklin, a Pentagon analyst, was charged with providing classified information about potential attacks on American forces in Iraq to two employees of the American Israel Public Affairs Committee, a pro-Israel lobbying group.[172] He pled guilty, but claimed he did not want to hurt the United States; rather, he thought the lobbyists to whom he gave the information would advocate for his position with the Administration.[173]

b. Avoiding Better Statutory Protections

These criminal prosecutions present the most public and vivid indication of Obama's strong views regarding those considered to have "leaked" classified information to the media. However, it could be argued that these present isolated cases involving relatively few individuals.[174] Indeed, counterexamples exist in which the Obama DOJ dropped charges or investigations against individuals accused by the Bush Administration of improperly disclosing classified information. In 2009, the DOJ approved the recommendation from career prosecutors to withdraw charges against Steven J. Rosen and Keith Weissman,[175] who the Bush Administration had accused of receiving classified information from Lawrence Franklin, discussed

171. United States v. Morison, 844 F.2d 1057, 1060-61 (4th Cir. 1988); Kitrosser, *supra* note 170, at 899. President Clinton later pardoned Mr. Morison. *See* Eric Lichtblau & David Johnston, *Use of Espionage Law in Secrets Case Troubles Analysts*, N.Y. TIMES, Aug. 6, 2005, at A10.

172. *See* David Johnston & Eric Lichtblau, *Analyst Charged with Disclosing Military Secrets*, N.Y. TIMES, May 5, 2005, at A1.

173. *See* Lee, *supra* note 170, at 1482; Scott Shane & David Johnston, *Pro-Israel Lobbying Group Roiled by Prosecution of Two Ex-Officials*, N.Y. TIMES, Mar. 5, 2006, § 1, at 21. The judge sentenced Franklin to twelve and a half years in prison, *see* Lee, *supra* note 170, at 1486, Shane & Johnston, *supra*; however, the court subsequently reduced the sentence to ten months of home detention, *see* Gerstein, *supra* note 8; Shane, *supra* note 132.

174. Indeed, one news report asserted that the "scattered" way in which the six cases developed "support the notion that they were not the result of a top-down policy." Scott Shane & Charlie Savage, *Administration Took Accidental Path to Setting Record in Leak Cases*, N.Y. TIMES, June 19, 2012, at A14. In the same article, however, the reporters quoted Eric Holder, the Attorney General, defending the DOJ against criticism that it was not investigating leaks sufficiently by telling the Senate Judiciary Committee that, "We have tried more leak cases-brought more leak cases during the course of this administration than any other administration." *Id.* The reporters also note that the President is promoting his prosecution record "as a political asset." *Id.* One other explanation for the increased prosecution could be that better technology makes the leakers easier to track down through email and cell phone records. *Id.*

175. Neil A. Lewis & David Johnston, *U.S. to Drop Spy Case Against Pro-Israel Lobbyists*, N.Y. TIMES, May 1, 2009, at A11. The prosecutors claimed that the judge had issued rulings making the case to difficult to prosecute. *See id*. For example, the judge rejected the prosecutors' attempt to conceal classified information at trial, which would force the government to disclose it publicly. *See id*.; *see also* Shane & Johnston, *supra* note 173 ("Some legal experts say the prosecution threatens political and press freedom, making a felony of the commerce in information and ideas that is Washington's lifeblood. Federal prosecutors are using the Espionage Act for the first time against Americans who are not government officials, do not have a security clearance and, by all indications, are not a part of a foreign spy operation.").

above, and giving it to a reporter and an Israeli diplomat.[176] In 2011, Obama's DOJ also dropped investigations of intelligence community employees who admitted giving *New York Times'* reporters information that helped the *Times* expose Bush's domestic wiretapping program.[177]

Given the inherent distinctions that can be made among individual prosecutions, perhaps the Obama Administration's stance regarding enhanced statutory protections for whistleblowers provides a more compelling example of its nuanced approach to national security whistleblowing. For years, whistleblower advocates and their allies in Congress supported legislation aimed at fixing numerous loopholes and defects in the primary legislation affecting federal government whistleblowers, the Whistleblower Protection Act.[178] In 2007, the House of Representatives passed H.R. 985 with an overwhelming bipartisan majority, 331-94.[179] The bill, called the Whistleblower Protection Enhancement Act of 2007 (WPEA), contained numerous improvements for federal whistleblowers, including access to jury trials in federal court and protections for a broad range of disclosures about government misconduct.[180] Importantly, H.R. 985 also provided new rights and protections to national security whistleblowers, who typically do not receive statutory protection and often must rely on internal agency administrative procedures to remedy any retaliation they experience for blowing the whistle.[181] Among other things, H.R. 985 protected national security whistleblowers who make disclosures about misconduct to a broad range of congressional and executive branch officials, and it allowed employees to bring claims of retaliation to federal court[182] – a process whistleblower advocates have claimed necessary to give full due process rights to government whistleblowers.[183] Additionally, the legislation barred revoking an

176. *See* Shane & Johnston, *supra* note 173.

177. *See* Charlie Savage, *No Prosecution Seen for Official in N.S.A. Leak*, N.Y. TIMES, April 27, 2011, at A17.

178. *See, e.g.*, S. REP. NO. 111-101, at 38 (2009) (detailing legislative attempts to pass improvements to the WPA).

179. *See* Final Vote Results for Roll Call 153 (Mar. 14, 2007), *available at* <http://clerk.house.gov/evs/2007/roll153.xml>. Two hundred twenty-nine Democrats and 102 Republicans voted in favor of the bill on March 14, 2007. *See id*.

180. *See* H.R. 985, 110th Cong. § 10 (2007).

181. I discuss the law currently affecting national security whistleblowers in more detail in Part III.B., *infra*.

182. *See* H.R. 985, 110th Cong. § 10 (2007). The protected disclosures would have mirrored the disclosures under the WPA, as amended by the WPEA, which would have greatly expanded the types of disclosures national security whistleblowers could make without fear of retaliation.

183. *See* Press Release, Nat'l Whistleblowers Ctr., Major Reversal: House Cuts Whistleblower Jury Trials, (Nov. 3, 2011), *available at* <http://www.whistleblowers.org/index.php?option=com_content&task=view&id=1293&Itemid=178> ("Access to jury trials is a hallmark in all modern whistleblower laws and an absolutely essential provision to ensure that whistleblowers can have a fair hearing.").

employee's security clearance as retaliation for blowing the whistle[184] – a common form of retaliation currently not prohibited.[185] It also limited the use of the "state secrets privilege" in cases brought by whistleblowers,[186] likely in response to the Bush Administration's highly publicized use of the privilege to prevent an FBI whistleblower from bringing a claim in federal court.[187] The House bill required that a court resolve an issue on which the privilege is claimed in favor of the employee and also required the agency to submit a detailed report to Congress whenever it invoked the privilege.[188] By any measure, H.R. 985 would have dramatically improved the protections available to all federal government whistleblowers, specifically including national security whistleblowers.

As a candidate for President, Obama signed a declaration that he supported government whistleblower protections "under the framework of H.R. 985."[189] However, Obama's stance towards these provisions changed after he became President. Although H.R. 985 never became law,[190] in January 2009, the House attached to the stimulus bill measures identical to H.R. 985's national security whistleblower provisions.[191] President Obama did not demand that they remain part of the stimulus bill, and the Senate removed them before passing the legislation in February 2009, a month after Obama took office.[192] The next month, members in the House introduced federal government whistleblower legislation again, and it contained protections for national security whistleblowers identical to H.R. 985.[193]

184. *See* H.R. 985, 110th Cong. § 10 (2007).

185. *See* Hesse v. Dep't of State, 217 F.3d 1372, 1380 (Fed. Cir. 2000).

186. The state secrets privilege permits the government to withhold revealing military and state secrets during a civil trial. *See* United States v. Reynolds, 345 U.S. 1, 7 (1953).

187. *See* MELISSA GOODMAN ET AL., DISAVOWED: THE GOVERNMENT'S UNCHECKED RETALIATION AGAINST NATIONAL SECURITY WHISTLEBLOWERS 11 (2007) (discussing claim of Sibel Edmonds).

188. *See* H.R. 985, 110th Cong. § 10 (2007).

189. *See* R. Jeffrey Smith & Joby Warrick, *Obama, Gates at Odds Over Proposed Protections for National Security Whistleblowers*, WASH. POST, Feb. 18, 2009, at A3; *Candidate Surveys*, NAT'L WHISTLEBLOWERS CTR., <http://www.whistleblowers.org/index.php?option= com_content&task=view&id=29&Itemid=58> (last visited Apr. 17, 2012).

190. The Senate passed a companion bill, S. 274, but Congress never reconciled the two bills. Notably, S. 274 did not contain the added protections for national security whistleblowers. *See* S. 274, 110th Cong. (2007).

191. *See* H.R. 1, 111th Cong. § 1270 (2009); Brittany R. Ballenstedt, *House Backs Whistleblower Provision in Stimulus Bill*, GOVEXEC.COM (Jan. 28, 2009), <http://www.govexec.com/dailyfed/0109/012809b1.htm>.

192. *See* 156 CONG. REC. H8,974 (daily ed. Dec. 22, 2010) (Statement of Rep. Van Hollen) (noting that provisions of H.R. 1507 were "stripped out of the Recovery Act during the conference with the Senate"); Smith & Warrick, *supra* note 189 (noting that the national security whistleblower provisions were dropped from the stimulus bill "after Sen. Susan Collins (Maine) and other Republicans objected to their inclusion and the White House did not insist on it").

193. *See* Whistleblower Protection Enhancement Act of 2009, H.R. 1507, 111th Cong.

However, the Obama Administration indicated that it had reservations about the national security whistleblower provisions.[194] Indeed, in a committee hearing on the new bill, H.R. 1507, an Obama Administration representative, Rajesh De from DOJ, approved of many of the bill's improvements for whistleblowers generally, but objected to H.R. 1507's enhancements for national security whistleblowers.[195] De asserted that a provision permitting federal employees a chance to appeal to a federal court when an agency revoked the employee's security clearance was "inconsistent with the traditional deference afforded Executive Branch decision-making in this area."[196] De also objected to federal district court review of MSPB decisions regarding national security whistleblowers because of "the sensitive nature of the issues involved" with national security whistleblowers.[197] The Obama Administration instead endorsed retaliation protection for national security whistleblowers through administrative procedures located entirely within the executive branch.[198]

At the same time, the Senate considered S. 372, another version of the WPEA, and held hearings at which De provided substantially similar testimony on behalf of the Obama Administration.[199] In December 2009, a Senate committee endorsed S. 372, which provided for national security whistleblower protection through an administrative, rather than a judicial, process.[200] By providing some antiretaliation protection for national security whistleblowers, S. 372 potentially improved the current lack of any real protection;[201] however, the bill included significantly less robust procedural protections than the judicial review found in H.R. 1507 (and H.R. 985 before that).[202] The Senate committee specifically accepted the Obama Ad-

194. Joe Davidson, *Whistleblower Advocates Push for More from Obama*, WASH. POST, May 15, 2009, at A17.

195. *See Protecting the Public from Waste, Fraud and Abuse: Hearing on H.R. 1507, The Whistleblower Protection Enhancement Act of 2009 Before the H. Comm. on Oversight & Gov't Reform*, 111th Cong. 7 (2009) (statement of Rajesh De, Deputy Ass't Att'y Gen., Office of Legal Policy, Dep't of Justice) [hereinafter De House Statement], *available at* <http://democrats.oversight.house.gov/images/ stories/documents/20090513192835.pdf>.

196. *See id*. at 9-10.

197. *See id*. at 11.

198. *See id*. at 7-10.

199. *See Hearing on S. 372 - The Whistleblower Protection Enhancement Act of 2009 Before the S. Subcomm. on Oversight of Gov't Mgmt., the Fed. Workforce, & the Dist. of Columbia*, 111th Cong. 7 (2009) (statement of Rajesh De, Dep. Ass't Att'y Gen., Office of Legal Policy, Dep't of Justice), *available at* <http://www.justice.gov/olp/pdf/rajeshde-whistleblower-senate.pdf>.

200. *See* S. REP. NO. 111-101, at 76-80 (2009).

201. *See* discussion *infra* Part III.B. (discussing current legal regime affecting national security whistleblowers). The version of S. 372 originally introduced in the Senate did not contain any protections for national security whistleblowers. *See* 155 CONG. REC. S1435-38 (daily ed. Feb. 3, 2009) (providing text as introduced in Senate).

202. Instead, S. 372 required whistleblowers to appeal an employment decision to the agency head

ministration's position that an administrative process would "better protect national security information."[203] Moreover, unlike H.R. 1507, S. 372 did not contain any provisions related to the government's use of the state secrets privilege, nor did it provide for outside review of an agency decision to revoke an employee's security clearance.[204]

Given De's testimony at the House and Senate hearings on the two versions of the WPEA, some whistleblower advocates blamed Obama for abandoning the strong national security whistleblower provisions of H. 1507 for the weaker version in S. 372. Not only did the Obama Administration suggest the administrative protections as an alternative to the judicial remedy of H.R. 1507, but also it became clear that the White House and national security officials, who had long objected to strong protections for intelligence community employees, worked with the Senate committee to craft a compromise bill with the weaker provisions.[205] The National Whistleblowers Center lamented that S. 372's "bad" provisions concerning national security whistleblowers "have the tacit or express approval of the Obama Administration, which throughout this process has deferred to the views of the federal agency managers and heads of the intel agencies."[206] News reports also indicated that Obama officials even weakened protections for FBI whistleblowers initially,[207] although the bill ultimately passed by the Senate in December 2010 retained the FBI's current protections.[208]

(rather than to a more independent Inspector General), who could control the resulting investigation. *See* S. REP. NO. 111-101, at 70 (2009). As part of the investigation, the agency could submit *ex parte* information to the agency decision maker if "the agency determines that the interests of national security so warrant." *Id*. The whistleblower would have a limited ability to subpoena witnesses or to compel production of evidence. *See id*. A whistleblower could appeal the agency decision to an administrative board created by the new law; however, the board would not conduct a hearing and would be dependent on the record accumulated by the agency (the same agency accused of retaliation), including credibility determinations made by the agency. *See id*. at 71. The board proceedings would not need to be on the record nor even conducted by administrative law judges, and the board could not share any of the *ex parte* evidence with the whistleblower. *See id*. The board could award damages (capped at $300,000) but could not order reinstatement of the employee. *See id*. at 72. Finally, the bill would have permitted agencies to fire whistleblowers without any review whatsoever when the agency itself determines that national security requires it. *See id*. at 73.

203. *Id*. at 30.

204. *See id*. at 79-80.

205. Tom LoBianco, *WH Sought to Weaken Law on Whistleblowing*, WASH. TIMES, Aug. 7, 2009, at A1; Smith & Warrick, *supra* note 189.

206. *See* David Colapinto, *Shine More Sunlight on S. 372*, WHISTLEBLOWERS PROT. BLOG (Mar. 10, 2010), <www.whistleblowersblog.org/2010/03/articles/whistleblowers-government-empl/terrorism/shine-more-sunlight-on-s-372/>.

207. *See* LoBianco, *supra* note 205; Kasie Hunt, *Critics Question Whistleblower Bill*, POLITICO (Mar. 9, 2010, 4:44 AM EDT), <http://www.politico.com/news/stories/0310/34105.html>.

208. *Compare* 156 CONG. REC. S8803 (daily ed. Dec. 10, 2010) (detailing S. Amdt. 4760 to S. 372, which did not include the FBI in the groups to which the administrative procedures were available under Section 201 and which the Senate passed on Dec. 10, 2010) *with* S. REP. NO. 111-101, at 68 (2009) (including FBI in groups affected by administrative procedures) *and* 156 Cong. REC. S8813 (daily ed.

As the legislative session for the 111th Congress wound to a close in December 2010, the House took up a measure identical to S. 372 rather than its own H.R. 1507, which had languished since the committee hearing eighteen months earlier. Yet, even the watered-down provisions for intelligence community whistleblowers proved to be too much for many Republicans,[209] and the House amended its version of S. 372 to delete all of the national security provisions.[210] A lone Senator put a hold on the bill when it returned to the Senate, and the 111th Congress ended without passing any version of the WPEA.[211] Professor Geoffrey Stone, Obama's former colleague at the University of Chicago Law School, complained that the Obama Administration "cooled to the idea" of a statute with enhanced federal employee whistleblower protection and "let it die" in the Senate.[212]

However, after several Senators reintroduced the Whistleblower Protection Enhancement Act in 2011, generally along the same lines as S. 372 from the previous Congress,[213] Obama publicly supported it.[214] This bill keeps many of the improvements to the WPA found in previous versions of the bill, but retains the administrative remedies for national security whistleblowers.[215] Interestingly, instead of detailing specific enforcement procedures like S. 372, the proposed legislation simply grants the President the power to provide for enforcement of its protections along the same lines as the WPA.[216] The administrative remedy seems to appeal to Obama; he has declared that even if Congress does not pass the WPEA, his Administration might use executive orders to implement what he can.[217]

Thus, the Obama Administration took a more nuanced approach to na-

Dec. 10, 2010) (reporting Committee's version to the Senate).

209. *See* 156 CONG. REC. H8974 (daily ed. Dec. 22, 2010) (Statement of Rep. Towns) ("I am disappointed that we could not come to an agreement with the Republican side on extending protections to employees in the Intelligence Community.").

210. *See* 156 CONG. REC. H8966-74 (daily ed. Dec. 22, 2010).

211. *House Republican Leadership Asked Senator to Place "Secret Hold" on Federal Whistleblower Bill*, GOV'T ACCOUNTABILITY PROJECT (Apr. 4, 2011), <http://www.whistleblower.org/press/press-release-archive/1037-house-republican-leadership-asked-senator-to-place-qsecret-holdq-on-federal-whistleblower-bill>.

212. Geoffrey R. Stone, *Our Untransparent President*, N.Y. TIMES, June 26, 2011, at A21.

213. *See* S. 743, 112th Cong (2011). On Oct. 19, 2011, the bill passed unanimously out of the Senate Committee on Homeland Security and Governmental Affairs. *See* Dylan Blaylock, *GAP Praises Senate Committee Vote on Whistleblower Protection Enhancement Act*, GOV'T ACCOUNTABILITY PROJECT (Oct. 19, 2011), <http://www.whistleblower.org/blog/31-2010/1556-gap-praises-senate-committee-vote-on-whistleblower-protection-enhancement-act>.

214. *See* Amanda Becker, *Obama Pushes for Whistle-Blower Bill*, ROLL CALL NEWS (Sept. 21, 2011), <http://www.rollcall.com/issues/57_32/Obama-Pushes-for-Whistle-Blower-Bill-208883-1.html?pos=hbtxt>.

215. *See* S. 743, 112th Cong. § 201 (2011).

216. *See id*.

217. *See* Becker, *supra* note 214.

tional security whistleblowing than candidate Obama's original endorsement of H.R. 985 would have indicated. Although the Obama Administration agreed the law should protect national security whistleblowers, it objected to providing them the same type of rights available to other whis-whistleblowers. Most dramatically, the Administration endorsed internal, administrative remedies instead of the House's preferred judicial remedies.

c. Journalist Subpoenas

The Obama Administration also focused on journalists who revealed classified information. James Risen presents one specific example. He co-authored the *New York Times* article that exposed the Bush Administration's domestic wiretapping program and wrote a book, *State of War*, which described a failed government attempt to undermine Iran's nuclear-weapons program.[218] Both the Bush and Obama Administrations investigated the sources for Risen's stories for years before Obama's prosecutors finally attempted to force Risen to testify against Jeffrey Sterling, the former C.I.A. officer charged with revealing national security information to Risen.[219] In fact, the Bush Administration dropped its attempt to subpoena Risen; however, the Obama prosecutors revived the effort by subpoenaing Risen's credit reports as well as his personal bank and telephone records as part of their investigation.[220] Issuing such subpoenas to a member of the press presents a host of thorny legal issues, including a potential clash with First Amendment protections. Accordingly, the Justice Department's own rules require the Attorney General to approve such subpoenas, demonstrating how seriously the Obama Administration pursued Sterling.[221] Indeed, the prosecutor's motion requesting the subpoena called Risen "an eyewitness to the serious crimes" at issue in the case, namely the disclosure of national security information.[222] Ultimately, a federal judge quashed the subpoena this past summer.[223]

218. *See* Jane Mayer, *James Risen's Subpoena*, THE NEW YORKER (May 24, 2011), <http://www.newyorker.com/online/blogs/newsdesk/2011/05/james-risens-subpoena.html>.

219. *See* Greenwald, *supra* note 8; Mayer, *supra* note 218.

220. *See* Josh Gerstein, *Feds Spy on Reporter in Leak Probe*, POLITICO (updated Feb. 25, 2011, 12:15 PM EST), <http://www.politico.com/news/stories/0211/50168.html>; Glenn Greenwald, *Climate of Fear: Jim Risen v. the Obama Administration*, SALON (June 23, 2011, 4:24 AM CDT), <http://www.salon.com/2011/06/23/risen_3/>.

221. *See* Mayer, *supra* note 218; Shane, *supra* note 132 ("By Justice Department rules, investigators may seek to question a journalist about his sources only after exhausting other options and with the approval of the attorney general. Subpoenas have been issued for reporters roughly once a year over the last two decades, according to Justice Department statistics, but such actions are invariably fought by news organizations and spark political debate over the First Amendment.").

222. *See* Mayer, *supra* note 218.

223. Greenwald, *supra* note 144.

The Risen subpoena reflects a policy reversal for Obama with regard to a reporter's right to protect sources, many of whom, of course, could be called whistleblowers. In 2007 as a U.S. Senator, Obama co-sponsored the Free Flow of Information Act, which would provide a federal journalist-source privilege allowing journalists to protect the confidentiality of their sources except in extreme circumstances, a right recognized by forty-nine states and the District of Columbia.[224] As a candidate for President, Obama promised to give protection to journalists from having to reveal their confidential sources.[225] However, as President, Obama demanded that exceptions exist to require a reporter to reveal a source in order to protect national security,[226] and he insisted that judges defer to the executive branch's judgment on whether national security would be affected.[227]

Not surprisingly, whistleblower advocates have raised strong objections to these events. Thomas Drake's lawyer, Jesselyn Radack, of the Government Accountability Project, called Obama's actions "brutal" and "a recipe for the slow poisoning of a democracy."[228] The Oscar-nominated director of a film about Daniel Ellsberg, of Pentagon Papers fame, claimed that Obama is the "worst President in terms of his record on whistleblowing."[229] Obama's proposed national security provisions for the WPEA provoked substantial criticism as well.[230] His former colleague, Professor

224. Stone, *supra* note 212. To overcome the privilege, the government would have to prove that disclosing the information would prevent significant harm to national security. *See id*.

225. *See* Charlie Savage, *White House Proposes Changes in Bill Protecting Reporters' Confidentiality*, N.Y. TIMES, Oct. 1, 2009, at A17; Clint Hendler, *A Change That's Hard to Believe In*, COLUM. JOURNALISM REV. (Oct. 2, 2009, 10:12 AM), <http://www.cjr.org/campaign_desk /a_change_thats_hard_to_believe.php> (providing transcript and quoting campaign speech by Obama from Apr. 15, 2008).

226. *See* Shane Harris, *Plugging the Leaks*, THE WASHINGTONIAN, Aug. 2010, at 33, *available at* <http://www.washingtonian.com/articles/people/plugging-the-leaks/>; Savage, *supra* note 225 ("The Administration this week sent to Congress sweeping revisions to a 'media shield' bill that would significantly weaken its protections against forcing reporters to testify" by not permitting protections for leaks involving "significant" harm to national security).

227. Stone, *supra* note 212.

228. Thomas Drake & Jesselyn Radack, *A Surprising War on Leaks Under Obama*, PHILLY.COM (Aug. 1, 2011), <http://articles.philly.com/2011-08-01/news/29838846_1_whistle-blowers-jesselyn-radack-obama>.

229. Ben Dowell, *Barack Obama Worst President for Whistleblowers, Says Film-maker*, THE GUARDIAN (June 9, 2011, 13:22 EDT), <http://www.guardian.co.uk/media/2011/jun/09/barack-obama-worst-president-for-whistleblowers>.

230. *See* Julia Davis, *Here Comes the Bride of Frankenstein*, EXAMINER.COM (Aug. 5, 2011), <http://www.examiner.com/homeland-security-in-los-angeles/here-comes-the-bride-of-frankenstein> ("The WPEA is replete with deceptive guillotines masquerading as haircut machines."); *Greenhouse: Senate Bill "Treats Whistleblowers as Second-class Citizens"*, Nat'l Whistleblowers Ctr. (Dec. 15, 2010), <http://www.whistleblowers.org/index.php?option=com_content&task=view&id=1166&Itemid=189> (noting that Bunnatine Greenhouse, an Army Corps of Engineers whistleblower who testified before Congress on whistleblower protections, stated that S. 372 "leaves national security whistleblowers out in the cold"); LoBianco, *supra* note 205 (quoting Tom Devine from the Government Accountability Project stating that "the White House changes [to the WPEA] created obstacles that could stymie

Stone, criticized some of Obama's moves in a *New York Times* editorial titled, "Our Untransparent President."[231]

The Obama Administration's actions provoked strong reactions from the media too. Glenn Greenwald from *Salon.com* called Obama's prosecutions "the most aggressive crusade to expose, punish and silence 'courageous and patriotic' whistleblowers by any President in decades."[232] *The Atlantic* complained that Obama is "waging a war on whistleblowers within the federal government,"[233] a sentiment others have echoed.[234]

However, the Obama Administration's involvement in the winding legislative path of the WPEA indicates a more nuanced attitude towards national security whistleblowers than demonstrated by the media hyperbole. Obama is not necessarily conducting a "war" on national security whistleblowers, because he has supported legislation protecting them. However, he may be conducting a battle for national security secrecy. He prioritized the protection of classified national security information by attempting to limit the ways in which intelligence community whistleblowers could disclose misconduct and the procedures they could invoke to remedy any retaliation they encounter. For Obama, administrative (rather than judicial) remedies for whistleblowers keep national security secrets within the executive branch and do not expose them to outsiders like Congress, judges, or the media. The criminal prosecutions and the Obama Administration's focus on "leaks" to the media supported the goal of national security secrecy. Obama appears to believe that not all whistleblowers are bad, just the ones who publicly disclose classified information when they blow the whistle. To put it bluntly, when it comes to national security, Obama would rather protect secrecy than protect whistleblowing.

This distinction between Obama's broad support for whistleblowing generally and his lack of support, often even condemnation, of whistleblowing about national security (or, more disparagingly, "leaking") deserves further exploration. Part III, below, analyzes the source for Obama's disdain for leaking and concludes that Obama's stance continues a long-

national security whistleblowers, such as a new review panel to hear complaints from intelligence employees who bring allegations of wrongdoing to light"); *Senate Passes S.372: A Bad Deal for Whistleblowers*, Nat'l Whistleblowers Ctr. (Dec. 11, 2010), <http://www.whistleblowers.org/index.php?option=com_content&task=view&id=1163&Itemid=71> (stating that S. 372 does "little to aid" national security whistleblowers).

231. *See* Stone, *supra* note 212.

232. Greenwald, *supra* note 8; *see also* Benjamin, *supra* note 155 (noting that the Obama Administration "is rapidly establishing a record as the most aggressive prosecutor of alleged government leakers in U.S. history").

233. *See* Estes, *supra* note 163.

234. *See, e.g.*, Greenwald, *supra* note 8; Horton, *supra* note 8.

standing presidential attitude toward national security whistleblowing based on constitutional separation of powers concerns. Obama, however, may be unique among his predecessors because of his strong support for other types of whistleblowers, making the distinction more apparent. Part IV evaluates the merits of Obama's singular distinction between national security whistleblowers and other types of whistleblowers.

III. WHISTLEBLOWING, NATIONAL SECURITY, AND THE SEPARATION OF POWERS

> Conflicts over secrecy . . . are conflicts over power: the power that comes through controlling the flow of information.
>
> *Sissela Bok (1982)*[235]

From the earliest days of the republic, the government has had to consider how to respond to executive branch employees who disclose misconduct in the national security arena. As Stephen Kohn, a well-known whistleblower advocate and lawyer, pointed out in *The New York Times*, Congress has encouraged people to report abuse and illegal conduct since the days of the Revolutionary War, when ten American sailors informed Congress that their commander treated prisoners of war inhumanly.[236] After the commander retaliated against the whistleblowers, Congress passed what Mr. Kohn called "America's first whistle-blower protection law":

> That it is the duty of all persons in the service of the United States, as well as all other inhabitants thereof, to give the earliest information to Congress or any other proper authority of any misconduct, frauds or misdemeanors committed by any officers or persons in the service of these states, which may come to their knowledge.[237]

Two centuries later Daniel Ellsberg released the Pentagon Papers to the *New York Times*, resulting in his prosecution under the Espionage Act. The landmark Supreme Court opinion that arose out of that case addressed the First Amendment rights of the *recipient* of classified information, but left open the question regarding the legal rights a whistleblower may have to disclose classified information about illegal or improper government conduct.[238] Most recently, the "War on Terror" that began after the September 11, 2001 attacks led to numerous government employees publicly disclosing information that touched on national security. These individuals

235. BOK, *supra* note 12, at 19.

236. *See* Stephen M. Kohn, *The Whistle-Blowers of 1777*, N.Y. TIMES, June 13, 2011, at A23.

237. *See id*.

238. *See* N.Y. Times v. United States, 403 U.S. 713, 714 (1971) (per curiam); Lee, *supra* note 170, at 1478 n.133.

believed they reported illegal or unethical government acts, such as the warrantless wiretapping by the National Security Agency,[239] the CIA renditions and water torture of suspected terrorists,[240] and the Abu Ghraib prisoner abuse.[241]

These examples and others follow a similar pattern and reinforce the definition of "national security whistleblower" I set out above: an executive branch employee who either works in the "intelligence community" or reveals classified information, or both.[242] Ellsberg met both definitions: he worked for the Department of Defense and revealed classified information.[243] Thomas Drake worked for the National Security Agency, but claims not to have disclosed anything classified.[244] Conversely, Thomas Tamm worked for the DOJ (not technically part of the "intelligence community"), but helped blow the whistle on the highly classified, but arguably illegal, NSA wiretapping program.[245] In the typical pattern, the national security employee discovers conduct the employee believes to be illegal or immoral, often relating to classified or confidential information, and tells Congress or the media about it.[246] Most recently, as noted above, the Obama Administration has ratcheted up government reaction to such actions by criminally prosecuting employees who arguably could be called whistleblowers.[247]

One explanation for Obama's intense reaction towards national securi-

239. *See* GOODMAN ET AL., *supra* note 187, at 14 (discussing case of Russell Tice); Michael P. Scharf & Colin T. McLaughlin, *On Terrorism and Whistleblowing*, 38 CASE W. RES. J. INT'L L. 567, 573-74 (2006); Michael Isikoff, *The Fed Who Blew the Whistle*, NEWSWEEK, Dec. 22, 2008, at 40, *available at* <http://www.thedailybeast.com/newsweek/2008/12/12/the-fed-who-blew-the-whistle.html> (discussing the case of Thomas Tamm who told the *New York Times* that the NSA was intercepting phone calls and emails in U.S. without judicial warrants).

240. *See* Scharf & McLaughlin, *supra* note 239, at 572-74; Jameel Jaffer & Larry Siems, *Honoring Those Who Said No*, N.Y. TIMES, Apr. 28, 2011, at 25.

241. *See* Scharf & McLaughlin, *supra* note 239, at 572-74; Jaffer & Siems, *supra* note 240.

242. *See supra* Part II.B.

243. *See* Daniel Ellsberg, *Secrecy and National Security Whistleblowing*, 77 SOC. RES. 773, 787-88 (2010).

244. *See* Mayer, *supra* note 8, at 55.

245. *See* Isikoff, *supra* note 239; Savage, *supra* note 177, at A17.

246. *See generally* LOUIS FISHER, CRS REPORT FOR CONGRESS: NATIONAL SECURITY WHISTLEBLOWERS (2005), *available at* <http://www.fas.org/sgp/crs/natsec/RL33215.pdf>; GOODMAN ET AL., *supra* note 187; Katel, *supra* note 32, at 265; Lee, *supra* note 170, at 1454-55. For example, Jesselyn Radack, a former FBI legal counsel, told a reporter about alleged "barbaric" treatment of John Walker Lindh, the "American Taliban," after his arrest, and claimed to have been retaliated against as a result. See Drake & Radack, *supra* note 228. Radack claims to have "warned the Justice Department against interrogating [Lindh] without an attorney" and "exposed the FBI's ethics violations in deciding to proceed, its barbaric treatment of him, and the mysterious disappearance of evidence of the warning from DOJ files." *Id.*; *see also* Eric Lichtblau, *Dispute Over Legal Advice Costs a Job and Snarls a Nomination*, N.Y. TIMES, May 22, 2003, at A15.

247. *See supra* text accompanying notes 141-73.

ty whistleblowers may be that such whistleblowers present a President with a unique dilemma. On the one hand, presidential decision making, particularly about national security, requires some amount of secrecy.[248] Executive branch officials need some private space in order to provide candid advice to the President and to vet proposals without the distorting impact of public scrutiny. Employees who blow the whistle undermine this process and destroy the ability of Presidents to keep what one author has called "necessary secrets."[249] On the other hand, the Constitution promotes government transparency and Congressional oversight of the executive branch.[250] Whistleblowers who expose misconduct play an important role in making the government transparent and assisting in inter-branch oversight. In other words, President Obama's nuanced approach to national security whistleblowing is part of a larger context related to these tensions that, at their core, result from the Constitution's separation of powers among co-equal branches of government.[251]

A. Valuing Oversight and Transparency over Secrecy

Whistleblowing, particularly by executive branch employees to Congress, brings to a head these arguments about the competing needs for executive secrecy and Congressional oversight. Such arguments have resulted in various attempts to balance these opposing interests depending on the circumstances surrounding the whistleblowing. Presidents of both political parties have long maintained that the chief executive can keep some secrets from Congress in order to do the President's job effectively.[252] Thomas Jef-

248. *See* BOK, *supra* note 12, at 191.

249. *See generally* GABRIEL SCHOENFELD, NECESSARY SECRETS: NATIONAL SECURITY, THE MEDIA, AND THE RULE OF LAW (2011).

250. *See* Heidi Kitrosser, *Secrecy and Separated Powers: Executive Privilege Revisited*, 92 IOWA L. REV. 489, 522 (2007).

251. *See* FISHER, *supra* note 246, at 2 ("Whistleblower activity is often viewed as a struggle between the executive and legislative branches.").

252. *See, e.g.*, OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY: H.R. 2701 – INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2010, at 1 (2009), *available at* <http://www.presidency.ucsb.edu/ws/index.php?pid=86389> (opposing changes to broaden executive branch reporting requirements to Congress because they "would undermine what the executive branch refers to as a 'fundamental compact between the Congress and the President' regarding the reporting of intelligence activities, 'an arrangement that for decades has balanced congressional oversight responsibilities with the President's responsibility to protect sensitive national security information"); Kathleen Clark, *"A New Era of Openness?": Disclosing Intelligence to Congress Under Obama*, 26 CONST. COMMENT. 313, 327-28 (2010) ("For decades, Presidents have claimed the right to control classified information and internal legal advice."); Katel, *supra* note 32, at 272 (quoting President George W. Bush official asserting that executive privilege doctrine includes keeping "intra-agency deliberative materials prepared for senior officers in executive departments" from Congress); Heidi Kitrosser, *Congressional Oversight of National Security Activities: Improving Information Funnels*, 29 CARDOZO L. REV. 1049, 1061 (2008).

ferson noted, "The Senate is not supposed by the Constitution to be acquainted with the concerns of the Executive Department. It was not intended that these should be communicated to them."[253] Indeed, some commentators have asserted that the President's ability to keep secrets presents one of the great strengths of the executive branch.[254] Professor Heidi Kitrosser examines these arguments and goes one step further by asserting that "[i]t is virtually inevitable that the President's constitutional capacity for secrecy expands dramatically over time"[255] due to the bureaucratic and technological realities of the office.[256] Obama's first signing statement, noted above, demonstrates that he takes the traditional executive's view that the President should be able to control federal employee communications to Congress "where such communications would be unlawful or would reveal information that is properly privileged or otherwise confidential."[257] In contrast, Congress and others have insisted that the legislative branch maintains constitutional authority to oversee all of the executive's actions,[258] including those related to national security. Congress, as a representative body, provides the best means for public oversight in a democracy, but only if Congress has access to information about the government's programs.[259]

Over the last century, each branch has erected legal bulwarks in this intra-governmental dispute between transparency and secrecy as it relates to executive branch employees providing information to Congress to assist

253. THOMAS JEFFERSON, *Opinion on the Powers of the Senate* (Apr. 24, 1790), *in* THE JEFFERSONIAN CYCLOPEDIA (John P. Foley ed., 1900), *quoted in* Glenn Sulmasy, *Panel: Secrecy and Barriers to Open Government, transcript from Symposium: Left Out in the Cold? The Chilling of Speech, Association, and the Press in Post-9/11 America*, 57 AM. U. L. REV. 1229, 1233 n.56 (2008).

254. *See, e.g.*, Kitrosser, *supra* note 170, at 887 (discussing writing of Alexander Hamilton and John Jay).

255. *See id*.

256. *See id*. at 887-89.

257. Statement by the President *supra* note 130. The law prohibited the use of appropriations to pay salaries of anyone who "interferes with or prohibits" communications between federal employees and Congress related to the employee's job or agency. Omnibus Appropriations Act of 2009, Pub. L. No. 111-8, 123 Stat. 684, Div. D, § 714(1) & 714(2).

258. *See* SEN. REP. NO. 111-101, at 27 (2009) (noting that a previous Senate committee had determined that a bill permitting intelligence community employees to disclose information to Congress was constitutional because "the regulation of national security information, while implicitly in the command authority of the President, is equally in the national security and foreign affairs authorities vested in Congress by the Constitution"); Katel, *supra* note 32, at 272 (quoting memo from Congressional Research Service attorney concluding that "Congress has a clear right and recognized prerogative . . . to receive from officers and employees of the agencies and departments of the United States accurate and truthful information regarding the federal programs and policies"); Kitrosser, *supra* note 252, at 1063-64.

259. *See* Morton H. Halperin & Daniel N. Hoffman, *Secrecy and the Right to Know*, 40 LAW & CONTEMP. PROBS. 132, 132 (1976) ("Congress, acting in behalf of the public, should first direct, and then oversee executive Administration.").

the legislative branch in its oversight responsibilities. For example, in 1902 and 1909, Presidents Roosevelt and Taft, respectively, issued "gag" orders in which they ordered executive branch employees to speak with Congress only if approved by their department head.[260] Congress became concerned that these orders would stifle its ability to oversee the executive branch, and, in 1912, it passed the Lloyd-LaFollette Act,[261] rejecting these orders and declaring that no one should interfere with the "right" of federal employees to talk to Congress.[262]

The debate continued in more modern times. When Congress passed the Inspector General Act of 1978,[263] it clashed with the President over whether Inspector Generals (IGs) must report findings of misconduct to Congress.[264] The House originally required IGs to report "particularly serious or flagrant" concerns to Congress within seven days after discovery and without obtaining approval from executive branch agency heads.[265] The Office of Legal Counsel objected because the provision potentially conflicted with the President's constitutional right to withhold information from Congress on the basis of executive privilege: the President claimed the authority to control whether and how executive branch IGs should report information to Congress.[266] The Senate version of the bill, which ultimately became law, compromised and required IGs to report "particularly serious or flagrant" concerns to agency heads, who should then provide them to Congress.[267] The Senate Report on the provision acknowledges, however, that "the President's constitutional privilege for confidential communications" may require an agency head to alter or delete information before reporting to Congress.[268] This awkward compromise between the two branches gives Congress some oversight over the most serious problems reported to IGs, but appears to leave the President with the power (through his agency heads) to conceal what he considers constitutionally privileged information.

260. *See* FISHER, *supra* note 246, at 2-3.

261. 37 Stat. 555, § 6 (1912). This language was carried forward and supplemented by the Civil Service Reform Act of l978 and is codified as permanent law. *See* 5 U.S.C. § 7211 (2006).

262. *See* FISHER, *supra* note 246, at 3; Thomas Newcomb, *In from the Cold: The Intelligence Community Whistleblower Protection Act of 1998*, 53 ADMIN. L. REV. 1235, 1239 n.10 (2001).

263. 5 U.S.C. app. § 5(d) (2006).

264. *See* Newcomb, *supra* note 262, at 1257-60.

265. *See id*. at 1258 (citing S. REP. NO. 95-1071, at 30-32, *summarized in pertinent part in*, H.R. REP. NO. 105-747, at 18-19 (1998)).

266. *See id*. (citing S. REP. NO. 95-1071, at 30-32, *summarized in pertinent part in*, H.R. REP. NO. 105-747, at 18-19 (1998)).

267. *See* 5 U.S.C. app. § 5(d); Newcomb, *supra* note 262, at 1258-59.

268. *See* Newcomb, *supra* note 262, at 1258-59 (citing S. REP. NO. 95-1071, at 31-32 (1978), *quoted in* H.R. REP. NO. 105-747, at 18-19 (1998)).

The quarrel extends beyond the IG process. Since the early 1980s, Presidents have required executive branch employees to sign nondisclosure agreements, while Congress has refused to provide any funds to enforce the agreements or to pay the salary of any executive branch official who prevents an employee from communicating with Congress.[269] Congress repeatedly passed provisions in appropriation bills that require the nondisclosure agreements both to prohibit employees from disclosing classified information *and* to clarify that the prohibition does not apply to disclosures to Congress or to law enforcement related to a substantial violation of law.[270]

Although President Obama supported whistleblower protections generally, he demonstrated a willingness to continue the arguments made by his predecessors for a strong executive privilege. For example, the Obama Administration refused to allow its social secretary to testify before Congress regarding security at a White House dinner because, as Obama's press secretary noted, "[b]ased on the separation of powers, staff here don't go to testify in front of Congress."[271]

Nevertheless, despite the gag orders and nondisclosure agreements, for the typical federal government whistleblower, the balance generally seems to be in favor of Congressional oversight and transparency because, at least on paper, the law protects most federal government employees who report most types of misconduct. The WPA provides remedies for many federal employees who suffer retaliation for disclosing government misconduct, such as illegal behavior, mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety.[272] Although administrative and court decisions have undermined these protections somewhat,[273] on paper, the WPA provides robust whistleblower protection because it protects disclosures on a wide range of misconduct to a broad group of people, including to an employee's supervisor, Congress, or even the press if necessary.[274] Moreover, entities independent of an employee's agency will investigate and adjudicate claims of retalia-

269. *See* FISHER, *supra* note 246, at 24-28.

270. *See id*. at 28.

271. Heidi Kitrosser, *National Security and the Article II Shell Game*, 26 CONST. COMMENT. 483, 519 (2010) (quoting Michael D. Shear, *Government Openness is Tested by Salahi Case*, WASH. POST., Dec. 4, 2009, at C7) (internal quotation marks omitted). In non-whistleblower contexts, Obama also asserted executive privilege positions eerily familiar to positions claimed by his predecessor, George W. Bush. *See generally* Stone, *supra* note 212. For example, President Obama continues to assert the state secrets privilege with regularity, even to defend actions taken by the Bush Administration related to the CIA renditions and the NSA wiretapping. *See id*.

272. *See* 5 U.S.C. § 2302(b)(8)(A) (2006).

273. *See* Devine Statement, *supra* note 18, at 13-19.

274. *See* FISHER, *supra* note 246, at 16-21.

tion, which ultimately could be heard by the judicial branch on appeal.[275]

B. Switching the Balance for National Security Whistleblowing

The laws affecting *national security* whistleblowers differ dramatically from these general provisions. As discussed in more detail below, employees may report misconduct related to national security to a more limited group of people, excluding most of Congress and all of the public. Moreover, less protection from retaliation exists, and the judicial branch has no oversight of retaliation claims because the claims are adjudicated administratively within the executive branch and often within the whistleblower's own agency, if at all.

1. The Classification System for National Security Information

A primary reason for the difference in the law's treatment of these types of whistleblowers relates to the different nature of the information being shared by the whistleblowers. A "national security whistleblower" often reveals "classified" information subject to special rules about its disclosure. The classification system for the federal government results from a Presidential executive order describing the various levels of secrecy that applies to certain types of information.[276] Presidents also control whether an individual receives a security clearance providing access to classified information.[277] As a result, whether information is classified, and therefore subject to tighter restrictions on whether and how it can be disclosed, "is almost entirely under the control of the executive branch."[278] Further, the executive branch can utilize criminal prosecution to enforce secrecy related to certain types of classified information.[279] For example, the Espionage

275. *See* 5 U.S.C. §§ 1201-04 (2006) (describing MSPB); *id*. §§ 1211-14 (describing OSC); *id*. § 7703(b)(1) (providing for review of MSPB decisions by the U.S. Court of Appeals for the Federal Circuit).

276. *See* Kitrosser, *supra* note 170, at 890-91 (describing the classification system); KEVIN KOSAR, CONGRESSIONAL RESEARCH SERV., CLASSIFIED INFORMATION POLICY AND EXECUTIVE ORDER 13526, at 3 (2010), *available at* <http://www.fas.org/sgp/crs/secrecy/R41528.pdf> ("[C]lassified information policy largely has been established through executive orders.").

277. *See* KOSAR, *supra* note 276, at 4 (noting that executive orders typically have defined "who in the federal government may classify information, what levels of classification and classification markings (e.g., 'top secret') may be used, who may access classified information, and how and when classified information is to be declassified"); *see also* Exec. Order No. 13,526, § 4.1, 75 Fed. Reg. 707 (Jan. 5, 2010) (limiting access to classified information to those who demonstrate eligibility to an agency head, sign a nondisclosure agreement, and have a need to know the information).

278. Kitrosser, *supra* note 170, at 890; *see also* KOSAR, *supra* note 276, at 5 (noting that Congress passed provision in the Fiscal Year 1995 Intelligence Authorization Act "allowing the President to have a lead role in devising classified information policy").

279. *See* JENNIFER K. ELSEA, CONGRESSIONAL RESEARCH SERV., CRIMINAL PROHIBITIONS ON THE PUBLICATION OF CLASSIFIED DEFENSE INFORMATION 10 (2011), *available at* <http://fpc.

Act of 1917, mentioned above, protects the secrecy of national defense information.[280] Presidents claim to derive the power to control the secrecy of national security information from the Constitution, which appoints the President as Commander in Chief.[281]

Supreme Court holdings provide part of the basis for this view as well. The Court determined in *Department of Navy v. Egan*,[282] that the Merit Systems Protection Board could not review the revocation of an employee's security clearance by an executive agency.[283] In so doing, the *Egan* Court waxed philosophically about the President's constitutional role as Commander in Chief under Article II and asserted that the

> authority to classify and control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to occupy a position in the Executive Branch that will give that person access to such information flows primarily from this constitutional investment of power in the President, and exists quite apart from any explicit congressional grant.[284]

Moreover, in separate cases, the Court determined that the President, in some circumstances, has a privilege to refuse disclosing to courts confidential communications regarding national security and military issues.[285] Additionally, in *Snepp v. United States*,[286] the Court noted that the government has a "compelling interest" in withholding national security information from unauthorized persons.[287]

However, the Constitution also provides Congress with oversight responsibilities, which leads to an inevitable conflict regarding when the

state.gov/documents/organization/148793.pdf> (detailing criminal penalties). It should be noted, however, that the U.S. does not have a criminal statute prohibiting the public disclosure of classified information generally – the statutes prohibit disclosing specific types of classified information. *See id*. In contrast, the United Kingdom has an "Official Secrets Act" that criminally penalizes the disclosure of any government secret. Congress passed a similar act in 2000 but President Clinton vetoed the bill. *See id*. at 25-26.

280. Espionage Act of 1917, 18 U.S.C. §§ 793-99 (2006).

281. *See* U.S. CONST. art. II, § 2 cl. 1; *see also* JENNIFER K. ELSEA, CONGRESSIONAL RESEARCH SERV., THE PROTECTION OF CLASSIFIED INFORMATION: THE LEGAL FRAMEWORK 1 (2011), *available at* <http://www.fas.org/sgp/crs/secrecy/RS21900.pdf> (noting that Presidents, including President Obama, cite constitutional authority when issuing an executive order related to classified information); Kitrosser, *supra* note 252, at 1061-62; Kitrosser, *supra* note 271, at 507; Newcomb, *supra* note 262, at 1239-40; Sulmasy, *supra* note 253, at 1233 ("[T]he founders, as well as many modern administrators in both the twentieth and twenty-first centuries, have strongly insisted that the media, the citizenry, and even Congress are presumptively not privy to most wartime secrets and intelligence activities.").

282. 484 U.S. 518 (1988).

283. *Id*. at 530.

284. *Id*. at 527.

285. *See* United States v. Nixon, 418 U.S. 683, 705 (1974); United States v. Reynolds, 345 U.S. 1, 10 (1953).

286. 444 U.S. 507 (1980).

287. *See id*. at 509 n.3.

President must provide national security information to Congress.[288] Interestingly, none of the Court's rulings provides the answer to whether the Constitution permits the President to withhold national security information from *Congress* – as compared to the prohibitions against disclosure to the public generally.[289] *Egan* dealt with whether an executive agency had authority to question the security clearance judgment of another executive agency, importantly noting that the Executive Branch has authority in military and national security affairs, "unless Congress specifically has provided otherwise."[290] *Reynolds* and *Nixon* addressed executive privilege in the context of revealing national security information to litigants and courts, not Congress.[291] *Snepp* held only that the CIA's contractual requirement that a former CIA agent obtain approval before publishing material related to the CIA was a reasonable way for the CIA to protect its interest in maintaining the "secrecy of information important to our national security."[292] Thus, the question of how much information Congress can demand from the President regarding national security remains somewhat of an open question as a constitutional matter.

The Security Act of 1947 resolves some of this conflict through a delicate and complicated arrangement that details when the executive branch must share classified information with Congress. Under the Act, the President, the Director of National Intelligence, and the intelligence agency heads must brief Congressional intelligence committees about "intelligence activities" and "any significant anticipated intelligence activity."[293] Additionally, a smaller group of congressional members, the so-called "Gang of Eight,"[294] receive executive briefings on "covert operations," when the President considers it "essential . . . to meet extraordinary circumstances

288. *See* Kitrosser, *supra* note 250, at 522 (summarizing arguments that Congress has a constitutional role in checking the President's secrecy-keeping powers).

289. *See* ELSEA, *supra* note 281, at 1 ("The Supreme Court has never directly addressed the extent to which Congress may constrain the executive branch's power in this area.").

290. *See* Dep't of Navy v. Egan, 484 U.S. 518, 530 (1988); *see also* FISHER, *supra* note 246, at 24 (arguing that *Egan* was based on statutory, not constitutional, framework and that Congress has authority to legislate about scope of security clearances).

291. *See* United States v. Nixon, 418 U.S. 683, 705 (1974); United States v. Reynolds, 345 U.S. 1, 10 (1953). Moreover, *Reynolds* specifically dealt with executive privilege as an *evidentiary* doctrine, not a Constitutional requirement. *See Reynolds*, 345 U.S. at 6-7.

292. Snepp v. United States, 444 U.S. 507, 509 n.3 (1980).

293. 50 U.S.C. § 413(a)(1) (2006) (President); *id*. § 413a(a)(1) (Director of National Intelligence and agency heads).

294. *See* Kitrosser, *supra* note 252, at 1053 (noting that the Gang of Eight consists of "the chairmen and ranking minority members of the congressional intelligence committees, the Speaker and minority leader of the House of Representatives, and the majority and minority leaders of the Senate" and quoting Heidi Kitrosser, *Macro-Transparency as Structural Directive: A Look a the NSA Surveillance Controversy*, 91 MINN. L. REV. 1163, 1204 nn.252-56 and accompanying text (2007)) (internal quotation marks omitted).

affecting vital interests of the United States."[295] The arrangement becomes complicated because congressional aides and staff members may not have the proper security clearances (controlled by the executive branch) to receive the information. Also, although congressional members may receive classified information, the law prohibits them from disclosing the information publicly, just as it would anyone else.[296]

National security whistleblowers upset this arrangement because they potentially circumvent these statutory procedures. They might give classified information to congressional aides who do not have appropriate clearance or to congressional members who do not sit on the applicable committees entitled to the information under the Security Act. Moreover, the executive branch traditionally has controlled when and how it conducts such security briefings, procedures undermined by an unauthorized whistleblower. National security whistleblowers run into even greater problems if they disclose classified information publicly (as opposed to Congress), because such disclosure could subject them to employment sanctions, such as dismissal,[297] to civil penalties, and in some cases make them criminally liable under statutes like the Espionage Act.[298]

Thus, whenever Congress insisted on receiving national security information from executive branch employees directly, without control by executive branch officials, Presidents have raised separation of powers objections. For example, in 1996, the Office of Legal Counsel (OLC) concluded that separation of powers principles prevented Congress from providing executive branch employees a "right" to disclose national security information to Congress or anyone else, which in the Administration's view nullified the Lloyd-LaFollette Act.[299] As noted in the OLC's memo on this topic,

> the President's role as Commander in Chief, head of the Executive Branch, and sole organ of the Nation in its external relations require that he have ultimate and unimpeded authority over the collection, retention and dissemination of intelligence and other national security information in the Executive Branch. There is no exception to this principle for those disseminations that would be made to Congress or its members.[300]

295. 50 U.S.C. § 413b(c)(2).

296. *See* Stephen I. Vladeck, *The Espionage Act and National Security Whistleblowing After* Garcetti, 57 AM. U. L. REV. 1531, 1545 (2008).

297. Exec. Order No. 13,526, § 5.5, 75 Fed. Reg. 707 (Jan. 5, 2010) (stating that violating government security regulations may result in "reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation").

298. *See* ELSEA, *supra* note 281, at 11; Vladeck, *supra* note 296, at 1536-37.

299. *See* Newcomb, *supra* note 262, at 1239-40.

300. Memorandum from Christopher H. Schroeder, Acting Assistant Attorney General, Office of

Congress, of course, often disagrees, as in 1997 when it passed an Intelligence Authorization bill with a section stating that "[i]t is the sense of Congress that Members of Congress have equal standing with officials of the Executive Branch to receive classified information so that Congress may carry out its oversight responsibilities under the Constitution."[301] Other experts, such as Dr. Louis Fisher, the Senior Specialist on Separation of Powers from the Congressional Research Service, agree with Congress because the Constitution does not explicitly provide for how national security information should be regulated.[302] Instead, both Congress and the President have implied powers related to national security, which means that they "share constitutional authority to regulate national security information."[303]

Like his predecessors, President Obama used separation of powers arguments to justify keeping from Congress secrets related to national security. His Administration objected to congressional proposals to require the executive branch to give certain information related to national security to the full congressional intelligence committees, which would change the current requirement to notify only the so-called "Gang of Eight" Congressional leaders from both parties.[304] Moreover, Obama threatened to veto a revised proposal that would give only generalized information to the intelligence committees, such as informing the committees that more details were provided to the Gang of Eight.[305]

Obama's Administration also cited separation of powers concerns when testifying to the House of Representatives about the WPEA, which would have provided substantial new rights to national security whistleblowers, telling the committee that, although the Administration supported whistleblower rights generally, "we must preserve the President's constitutional responsibility with regard to the security of national security information."[306] The provisions of the WPEA that would have permitted federal

Legal Counsel, to Michael J. O'Neil, General Counsel, CIA (Nov. 26, 1996), *quoted in* Newcomb, *supra* note 262, at 1240.

301. The Intelligence Authorization Act for Fiscal Year 1998, Pub. L. No. 105-107, § 306, 111 Stat. 2248, 2252 (1997), *quoted in* Newcomb, *supra* note 262, at 1241-42 n.17; *see also* FISHER, *supra* note 246, at 41 ("Congress has never accepted the theory that the President has exclusive, ultimate, and unimpeded authority over the collection, retention, and dissemination of national security information.").

302. S. REP. NO. 105-165, at 4-5 (1998) *quoted in* Newcomb, *supra* note 262, at 1243.

303. *Id*.; *see also* Halperin & Hoffman, *supra* note 259, at 153 (arguing that the constitutional powers granted to Congress and the President are "independent but concurrent efforts by the respective branches on behalf of national security interests").

304. *See* Kitrosser, *supra* note 271, at 519.

305. *See id*.

306. De House Statement, *supra* note 195, at 3.

employees to reveal classified information when they believed it related to wrongdoing "would unconstitutionally restrict the ability of the President to protect from disclosure information that would harm national security."[307]

As a result of the heightened separation of powers concerns regarding national security, the law affecting whistleblowers who disclose problems related to national security differs dramatically from the law for other types of whistleblowers. National security employees receive limited antiretaliation protection and may disclose only a narrow range of wrongdoing to a restricted group of individuals.[308]

2. Limited Antiretaliation Protection

The most obvious difference between antiretaliation protection for national security whistleblowers and other whistleblowers relates to the coverage of the WPA. Specifically, the WPA does not protect employees of agencies related to national security, such as the FBI, the CIA, and the National Security Agency.[309] The Act also exempts from coverage employees who possess classified information or, even more broadly, who work in government agencies that likely deal with national security whether or not they handle classified information.[310] Whether they blow the whistle on national security issues or something more mundane, like gross mismanagement, these employees do not receive the WPA-provided right to investigation by the Office of Special Counsel and adjudication in front of the Merit Systems Protection Board, an independent agency outside of their home agency.

Moreover, even employees covered by the WPA who disclose information related to national security may not find much protection because

307. *See id*. at 8.

308. This section will describe generally the whistleblower provisions related to national security. For a more detailed description of the variety of laws affecting national security whistleblowers, please refer to FISHER, *supra* note 246, GOODMAN, ET AL., *supra* note 187, Vladeck, *supra* note 296, and Melissa Khemani, *The Protection of National Security Whistleblowers: Imperative but Impossible: A Critical Appraisal of the Scope and Adequacy of Whistleblower Protection Laws for National Security Whistleblowers* (May 30, 2009) (unpublished manuscript), *available at* <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1412112>.

309. *See* 5 U.S.C. § 2302(a)(2)(C)(ii) (2006) (excluding from WPA coverage "the Federal Bureau of Investigation, the Central Intelligence Agency, the Defense Intelligence Agency, the National Geospatial-Intelligence Agency, the National Security Agency, and, as determined by the President, any Executive agency or unit thereof the principal function of which is the conduct of foreign intelligence or counterintelligence activities").

310. In particular, the Act excludes employees in positions that are "excepted from the competitive service because of its confidential, policy-determining, policy-making, or policy-advocating character" or "based on a determination by the President that it is necessary and warranted by conditions of good Administration." *Id*. § 2303(a)(2)(B). Note that these exceptions explicitly do not include employees of the Department of Homeland Security or the Department of Energy.

the WPA limits disclosures about classified information by not protecting disclosures "specifically prohibited by law" or "specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs."[311] Typically, this means information designated as "classified" by Executive Order and prohibited by statute from being revealed publicly.[312] Employees can make these types of disclosures only to an IG or the Office of Special Counsel,[313] or perhaps Congress if the Congressional member receiving the information sits on the appropriate committee.[314] The legislative history of the CSRA and the WPA provide some evidence that Congress never intended to protect whistleblowers "who disclose information which is classified or prohibited by statute from disclosure."[315] Also, the WPA does not prohibit revocation of an employee's security clearance, which almost certainly would be revoked once an executive branch agency discovered the employee's whistleblowing.[316] Because many jobs require a certain security clearance, revoking a clearance often equates to a dismissal and leaves the employee with no protection from retaliation.[317]

Some national security whistleblowers may receive antiretaliation protections from other statutes and regulations; however they often provide protections inferior to those provided by the WPA to non-national security whistleblowers. For example, FBI employees who disclose misconduct[318] to various entities within the DOJ[319] may bring a claim through an internal

311. *See id*. § 2302(b)(8)(A)

312. *See* Vladeck, *supra* note 296, at 1537 (noting that the Espionage Act, 18 U.S.C. § 793(d) (2006), prohibits giving classified national security information "to any person not entitled to receive it").

313. *See* 5 U.S.C. § 2302(b)(8)(B).

314. *See id*. § 2302(b)(8) ("This subsection shall not be construed to authorize the withholding of information from the Congress or the taking of any personnel action against an employee who discloses information to the Congress.").

315. FISHER, *supra* note 246, at 7 (quoting S. REP. NO. 95-969, at 9 (1978)) (internal quotation marks omitted).

316. *See* Hesse v. Dep't of State, 217 F.3d 1372, 1380 (Fed. Cir. 2000). *Egan* does not address this issue because Congress amended the Civil Service Reform Act, upon which *Egan* was based, in 1989 and 1994, and the *Hesse* court considered whether Congress had "specifically" addressed the security clearance issue in those amendments, finding that it did not. *See id*. at 1377-80.

317. *See* S. REP. NO. 111-101, at 34 (2009) ("The effective result of the removal of an employee's security clearance or the denial of access to classified information typically is employment termination."); ELSEA, *supra* note 281, at 11.

318. The types of disclosures protected by this provision mirror the WPA's protected disclosures. *See* 5 U.S.C. § 2303(a) (2006).

319. The disclosures must be made to the Department's Office of Professional Responsibility, the IG, the FBI's Office of Professional Responsibility, the FBI Inspection Division Internal Investigations Section, the Attorney General, the Deputy Attorney General, the FBI Director or Deputy Director, or the highest ranking official in an FBI field office. *See* Whistleblower Protection for Federal Bureau of Investigation Employees, 28 C.F.R. § 27.1(a) (2011).

administrative process if they suffer retaliation because of the disclosure.[320] An administrative office within DOJ conducts an investigation of reprisal claims,[321] and the Director of the Office of Attorney Recruitment and Management (also located within DOJ) may conduct a hearing and award remedies if the employee demonstrates retaliation.[322] The Deputy Attorney General may review the Director's decision, but the regulations implementing the Act do not permit an appeal to court or even the Office of Special Counsel.[323] Although the standards utilized under the FBI's procedures appear similar to the WPA's standards, the entirely internal process can be problematic because of the lack of independence from the process's decision makers.[324] Moreover, the FBI provisions protect only disclosures made within the DOJ; an FBI agent who reports problems to Congress or the public will not receive protection from retaliation.[325]

The Military Whistleblower Protection Act (MWPA)[326] provides similarly limited protections by prohibiting retaliation against members of the military for lawful communications with Congress or an IG[327] as well as for making certain, defined protected disclosures within the military hierarchy.[328] As with the FBI protections, an internal administrative process adjudicates claims of retaliation, ultimately concluding with review by the Secretary of Defense.[329] The process remains entirely internal, and the Act also permits the Secretary of Defense to restrict IG investigations in certain intelligence and national security matters.[330] That said, the Department of Defense regulations adopt the whistleblower-friendly standards of the WPA and also improve upon the WPA's standards in one important re-

320. Although a statute authorizes the FBI protections, see 5 U.S.C. § 2303, administrative regulations detail the procedure and substantive remedies, see 28 C.F.R. Part 27 (2011).

321. *See* 28 C.F.R. § 27.3 (2011).

322. *See id*. § 27.4.

323. *See id*. § 27.5.

324. *But see* Valerie Caproni, *Panel: The Role of Whistleblowers to Facilitate Government Accountability*, 57 AM. U. L. REV. 1243, 1244 (2008) (arguing that the procedures offer a "fairly robust regulatory scheme to protect whistleblowers within the FBI").

325. *See* 28 C.F.R. § 27.1(a) (defining protected disclosure). While I call this process problematic, it did not trouble Valerie Caproni, the FBI's General Counsel in 2008, because "[t]here are enough options [for disclosure] that no employee should feel he or she is in the position of knowing horrible secrets of criminality and have no place to turn." Caproni, *supra* note 324, at 1245-46. Moreover, Ms. Caproni asserted that the DOJ will consider a disclosure made directly to Congress as "protected," even though it "thwarts the statutory scheme." *Id*. at 1248. The regulations, however, do not appear to require this position.

326. *See* 10 U.S.C. § 1034 (2006).

327. *See id*. § 1034(b)(1)(A).

328. *See id*. §§ 1034(b)(1)(B); 1034(c)(2) (defining protected disclosure similarly to the WPA).

329. *See id*. §§ 1034(c)-(g).

330. *See* 5 U.S.C. app. 3 § 8(b)(2) (2006).

spect: they permit a remedy for retaliation related to security clearances.[331]

Like many of the whistleblower protections detailed here, the MWPA arose out of a separation of powers dispute. In 1954, President Eisenhower refused to permit Defense Department employees to testify to Congress about conversations between executive branch employees.[332] The Attorney General and the DOJ issued legal memoranda claiming the Constitution permits the President to withhold information from Congress in the public interest.[333] Congress complained that the President was forcing Congress to "rely upon spoon-fed information from the President."[334] Ultimately, Congress passed the MWPA declaring that "No person may restrict any member of an armed force in communicating with a member of Congress, unless the communication is unlawful or violates a regulation necessary to the security of the United States,"[335] and subsequently added antiretaliation protections in 1988.[336]

Finally, national security whistleblowers likely have less protection under the First Amendment than other government employees. *Garcetti v. Ceballos*[337] held that the First Amendment does not protect government employees who speak out publicly "pursuant to their official duties."[338] Importantly, the Court also stated that "[r]estricting speech that owes its existence to a public employee's professional responsibilities does not infringe any liberties the employee might have enjoyed as a private citizen."[339] Based on this statement, Professor Stephen Vladeck and others concluded that this likely means that the First Amendment does not protect national security employees who disclose classified information, even if about a matter of public concern.[340] As Vladeck noted,

> *Garcetti* also appears to preclude First Amendment protections for any speech made by a government employee that would not have been possible if he were not a government employee, even if the speech itself is not made as part of the employee's official duties.

331. Dep't of Defense 5200.2-R, Dept of Defense Personnel Security Program, Subsection DL1.1.30.

332. *See* FISHER, *supra* note 246, at 22-23.

333. *See id*.

334. *See id*. at 23 (quoting CQ Almanac 740 (1956)) (internal quotation marks omitted).

335. 70A Stat. 80 (1956) (codified as amended at 10 U.S.C. § 1034 (2006)).

336. *See* FISHER, *supra* note 246, at 23.

337. 547 U.S. 410 (2006).

338. *Id*. at 421.

339. *Id*. at 421-22.

340. *See* Vladeck, *supra* note 296, at 1540; *see also* Lee, *supra* note 170, at 1473 (concluding that "insiders" who leak information will have little protection from the First Amendment); Jamie Sasser, *Silenced Citizens: The Post-*Garcetti *Landscape for Public Sector Employees Working in National Security*, 41 U. RICH. L. REV 759, 760 (2007) (reaching same conclusion as Vladeck).

> Where classified national security information is concerned, the stopping point of this logic is immediately clear: National security secrets are, by definition, information to which the average private citizen does not have access. Speech related to national security secrets, then, would seem to fall squarely within the category of speech Justice Kennedy identified in *Garcetti* as falling outside the First Amendment's umbrella.[341]

Construing *Garcetti* more narrowly might permit a national security whistleblower to blow the whistle as a citizen, by disclosing information to the public, such as through the media. However, Vladeck also relied on a 2007 D.C. Circuit opinion to point out that courts will be unlikely to uphold First Amendment protection for a disclosure made with knowledge that "it was unlawfully obtained or leaked."[342] Although a full analysis of *Garcetti*'s impact on the First Amendment rights of national security whistleblowers is beyond the scope of this Article,[343] at a minimum it would appear difficult for a national security whistleblower to claim constitutional protection for revealing classified information.

In sum, with constitutional protection questionable, retaliation protection for national security whistleblowers depends greatly upon the governmental agency for which one works. In the few agencies where statutes and regulations provide some protection, they rarely permit claims to be made outside of the employee's own agency or to be reviewed by a third-party, such as an independent board or a court. Moreover, the protections only extend to "lawful" disclosures of information, which because of the nature of the classification restrictions, do not permit national security whistleblowers to disclose misconduct related to classified information to most members of Congress or to the media.

3. Structural Disclosure Channels

To counterbalance this inferior antiretaliation protection and in order to have some oversight over the executive branch, Congress developed a variety of structural channels that whistleblowers can use to disclose misconduct. These channels permit some reporting internally to other executive branch officials or entities, and in one limited circumstance, to Congress. However, these channels neither give national security

341. Vladeck, *supra* note 296, at 1540.

342. *See id*. at 1540 n.50 (citing Boehner v. McDermott, 484 F.3d 573, 580-81 (D.C. Cir. 2007)).

343. Whether the First Amendment would protect a national security whistleblower is a topic that deserves its own article, which others have written. *See id*. at 1540 (concluding that First Amendment would not protect national security whistleblowers after *Garcetti v. Ceballos*, 547 U.S. 410 (2006)); *see also* Lee, *supra* note 170, at 1473 (concluding that "insiders" who leak information will have little protection from First Amendment); Sasser, *supra* note 340, at 760 (2007) (reaching same conclusion).

whistleblowers an unrestricted right to report to Congress nor permit them to disclose information to the general public.

The WPA provides a disclosure channel for employees to report misconduct to the Office of Special Counsel.[344] Typically, the OSC provides these reports to agency heads, who must then respond to the allegations with a written report that ultimately will be sent to the President and appropriate members of Congress.[345] The law, however, specifically exempts reports involving foreign intelligence or counterintelligence information, if the law or an Executive Order specifically prohibits the disclosure.[346] The OSC will send those restricted disclosures to the National Security Advisor and to Congressional intelligence committees, which ends the OSC's involvement in investigating the disclosure.[347]

In Part III.A., *supra*, I discussed the Inspector General Act of 1978, which provides a person within each agency to receive disclosures about the same types of information protected by the WPA: "a violation of law, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority or a substantial and specific danger to the public health and safety."[348] After investigating, the IG must report violations of federal criminal law to the Attorney General,[349] and "serious or flagrant problems, abuses, or deficiencies relating to the Administration of programs and operations of such establishment" to the agency head, who must report them to Congress within seven days.[350] Congress later instituted statutory IGs for the CIA[351] and the Department of Defense.[352] In 2010, Congress implemented an overarching IG for the entire intelligence community, charged with coordinating the IGs of each individual intelligence agency as well as conducting its own investigations.[353]

These various IG statutes, however, do not address some specific issues with regard to whistleblowing by members of the intelligence community. As with the WPA, for example, the IG Acts specifically exclude public disclosure of any information prohibited by law, such as classified

344. *See* 5 U.S.C. § 1213 (2006).
345. *See id.* §§ 1213(c); (d); (e).
346. *See id.* § 1213(j).
347. *See id.*
348. *See* 5 U.S.C. app. 3 § 7(a) (2006).
349. *See id*. § 4(d).
350. *See id*. § 5(d).
351. *See* 50 U.S.C. § 403q (2006).
352. *See* 5 U.S.C. app. 3 § 8 (2006 & Supp. IV 2010); Newcomb, *supra* note 262, at 1257.
353. *See* The Intelligence Authorization Act for Fiscal Year 2010, Pub. L. No. 111-259, § 405, 124 Stat. 2654 ((codified at 50 U.S.C. § 403-3h (Supp. IV 2010)).

information.[354] Moreover, although the IGs must provide semiannual reports to Congress and publicly,[355] nothing in the IG Acts provide executive branch employees the right to go directly to Congress, or to the public generally, with concerns about misconduct. In fact, the Act appears to permit the President or the head of an agency to refuse to provide classified information to Congress under the claim of executive privilege.[356] The IG Act for the Department of Defense makes this privilege clear by placing the IG under the "authority, direction, and control" of the Secretary of Defense when the IG engages in an investigation requiring access to information "the disclosure of which would constitute a serious threat to national security."[357] Furthermore, although sound in theory, the IG system does not completely eliminate the inherent conflict of the executive branch reviewing retaliation claims by its own employees, because a President or an agency head actually appoints, supervises, evaluates and can fire IGs.[358] After the initial IG Act passed, the most glaring problem with the IG system from Congress' perspective, however, could have been that, for some reason, the intelligence agency IGs simply did not use the "serious or flagrant" process, and Congress was not getting the information it needed from front-line intelligence agency employees.[359]

To address these limitations, Congress passed the Intelligence Community Whistleblower Protection Act of 1998 (ICWPA),[360] which provides a way for national security whistleblowers to report misconduct related to an "urgent concern." (Because the new Intelligence Community IG statute contains identical provisions,[361] for convenience, I will refer to them collectively as the ICWPA.) These statutes define an "urgent concern" as

(A) A serious or flagrant problem, abuse, violation of law or Executive

354. *See* 5 U.S.C. app. 3 § 5(e)(1).

355. *See id*. § 5(a) (Congress); § 5(c) (public). The CIA IG must provide a classified report to Congress. *See* 50 U.S.C. § 403q(d)(1).

356. *See* Newcomb, *supra* note 262, at 1258-59.

357. *See* 5 U.S.C. § 8(b)(1)(E) (2006). The Act also gives this same control when the investigation requires access to "sensitive operational plans," "intelligence matters," "counterintelligence matters," and "ongoing criminal investigations by other administrative units of the Department of Defense related to national security." *See id*. §§ 8(b)(1)(A)-(D). The Central Intelligence Agency Act of 1949, which was amended to add a statutory IG for the CIA, has a similar provision permitting the Director of the CIA to prohibit an IG investigation when the "prohibition is necessary to protect vital national security interests." 50 U.S.C. § 403q(b)(3). A similar provision restricts the new IG for the Intelligence Community. *See* 50 U.S.C. § 403-3h(f)(1).

358. *See* PROJECT ON GOV'T OVERSIGHT, *supra* note 31, at 7.

359. *See* Newcomb, *supra* note 262, at 1256 n.61 (quoting a letter from Representative Porter Goss to the heads of the intelligence agencies in which Goss makes this assertion).

360. *See* The Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 701, 112 Stat. 2396 (1998) (containing the ICWPA, codified at 5 U.S.C. app. 3 § 8H); *id*. § 702 (containing an identical provision applicable to the CIA and codified at 50 U.S.C. § 403q(d)(5)).

361. *See* 50 U.S.C. § 403-3h(k)(5).

> order, or deficiency relating to the funding, administration, or operations of an intelligence activity involving classified information, but does not include differences of opinions concerning public policy matters; (B) A false statement to Congress, or a willful withholding from Congress, on an issue of material fact relating to the funding, Administration, or operation of an intelligence activity; (C) An action, including a personnel action described in section 2302(a)(2)(A) of title 5, United States Code, constituting reprisal or threat of reprisal prohibited under subsection (7)(c) in response to an employee's reporting an urgent concern in accordance with this section.[362]

Before reporting this urgent concern to Congress, an employee of the intelligence community[363] must disclose the information to the agency's IG or to the Intelligence Community IG. The IG must investigate an "urgent concern" report within fourteen days, determine whether it is credible, and if it is, give the information to the head of the agency or the Director of National Intelligence, [364] who must give it to Congress within seven days.[365] Importantly, the ICWPA permits the employee to report to Congress directly if the IG does not find the employee's report credible or does not provide it to the agency head accurately.[366] However, in that instance, the employee must tell the agency head about the employee's plan to report to Congress, the employee must follow any instruction from the agency head on how to contact Congress "in accordance with appropriate security practices," and the employee may only give the information to Congressional intelligence committees.[367]

Interestingly, these acts give the appearance of protecting from retaliation employees who report to an IG. For example, the Inspector General Act of 1978 states that no one shall "take or threaten to take any action against any employee as a reprisal for making a complaint or disclosing information to an IG, unless the complaint was made or the information disclosed with the knowledge that it was false or with willful disregard for its truth or falsity."[368] Identical provisions appear in the CIA IG provision[369] and in the new IG act for the Intelligence Community.[370] However, despite such prohibitions, these Acts do not appear to permit employees to file a

362. 5 U.S.C. app. 3 § 8H(h)(1).

363. The ICWPA covers a wide variety of intelligence agencies, including the CIA, the Department of Defense, the FBI, and those designated by the President as having its principal function conducting foreign intelligence or counterintelligence activities. *See* 5 U.S.C. app. 3 § 8H(a)(1).

364. *See id*. § 8H(b).

365. *See id*. § 8H(c).

366. *See id*. § 8H(d)(1).

367. *Id*. § 8H(d)(2).

368. *Id*. § 7(c).

369. *See* 50 U.S.C. § 403q(e)(3)(B) (Supp. IV 2010).

370. *See id*. § 403-3h(g)(3)(B).

grievance or a cause of action for such retaliation, which obviously limits the protections' effectiveness.

The ICWPA and the Inspectors General process differ greatly from the whistleblower provisions available to non-security employees under the WPA. Most obviously, they do not provide any substantive protection from retaliation, which likely reduces an employee's willingness to disclose wrongdoing and therefore gives the President almost unchecked authority to keep national security information secret from Congress. Moreover, the ICWPA only addresses misconduct that meets the definition of an "urgent concern," meaning that Congress likely will not hear from intelligence community employees regarding matters that, although important, do not rise to the level of an "urgent concern."[371] Further, under the WPA, any covered executive branch employee can make a protected disclosure to anyone in Congress, while the disclosure options for national security whistleblowers are much more restricted. These differences relate specifically to the separation of powers concerns discussed above.

For example, when negotiating the passage of the ICWPA, the legislative and executive branches disagreed on whether the act should include a "holdback provision," allowing IGs and agency heads to keep whistleblower information from Congress in extraordinary circumstances to "protect vital law enforcement, foreign affairs, or national security interests."[372] Similarly to the debate in 1978 over the IG Act,[373] the Clinton Administration in 1998 asserted that the presidential privilege required a holdback provision.[374] Congress demurred and chose to leave such extraordinary circumstances to be resolved on a case-by-case basis "through personal communication" between agency heads and congressional leaders.[375]

Yet, even this compromise was laced with indications that each branch maintained its constitutional authority of either oversight, in the case of Congress, or secrecy, in the case of the President. In its legislative findings, Congress specified that the Constitution required it to "serve as a check on the executive branch," with the responsibility to find out about wrongdoing in the executive branch generally and in the intelligence community more specifically.[376] It further declared that "no basis in law exists for requiring

371. *See* Sasser, *supra* note 340, at 784.

372. Newcomb, *supra* note 262, at 1262 (quoting H.R. 3829, 105th Cong. § 2(a)(E) (1998)) (internal quotation marks omitted).

373. *See supra* text accompanying notes 263-68.

374. *See* Newcomb, *supra* note 262, at 1262.

375. *See id*. at 1264 (quoting H.R. REP. NO. 105-747, at 14 (1998)) (internal quotation marks omitted).

376. *See* Pub. L. No. 105-272, title VII, § 701(b), 112 Stat. 2413 (1998).

prior authorization of disclosures" by the executive branch before an employee could report misconduct to Congress.[377] In contrast, President Clinton issued a statement when he signed the bill noting that the "Act does not constrain my constitutional authority to review and, if appropriate, control disclosure of certain classified information to Congress. . . . The Constitution vests the President with the authority to control disclosure of information when necessary for the discharge of his constitutional responsibilities."[378] In other words, as Thomas Newcomb noted, Congress labeled this compromise "comity," while the President labeled it a constitutional prerogative.[379]

Not surprisingly, the separation of powers issue played a role when Congress recommended the creation of an IG for all of the combined intelligence agencies, with reporting requirements similar to the ICWPA. Similar to President Clinton's reaction to the ICWPA, President Obama objected to reporting requirements imposed upon the new IG and the Director of National Intelligence based on the same constitutional grounds that President Clinton objected to with the ICWPA.[380] Obama not only specifically referenced President Clinton's signing statement for the ICWPA, but also he repeated that he did not view the disclosure requirements as mandating "disclosure of privileged or otherwise confidential law enforcement information."[381] The Obama Administration stated that while it supported expansion of retaliation protections for intelligence community whistleblowers, it also did not want any bill interpreted "to constrain the President's constitutional authority to review and, if appropriate, control disclosure of certain classified information."[382] The Obama Administration stated that it preferred to work out a compromise with Congress on protections for intelligence community whistleblowers through the WPEA in order to address "constitutional and other concerns."[383]

In sum, for national security whistleblowers, the law's balance weighs in favor of secrecy. National security whistleblowers receive less robust

377. *See id*.

378. William J. Clinton, Statement on Signing the Intelligence Authorization Act for Fiscal Year 1999, Oct. 20, 1998, *available at* Gerhard Peters & John T. Woolley, THE AMERICAN PRESIDENCY PROJECT, <http://www.presidency.ucsb.edu/ws/?pid=55116>.

379. *See* Newcomb, *supra* note 262, at 1265-67.

380. *See supra* discussion accompanying notes 372-78; Barack Obama, Statement on Signing the Intelligence Authorization Act for Fiscal Year 2010, Oct. 7, 2010, *available at* Gerhard Peters & John T. Woolley, THE AMERICAN PRESIDENCY PROJECT, <http://www.presidency.ucsb.edu/ws/?pid=88549> (referring specifically to President Clinton's signing statement).

381. *See* Obama, *supra* note 380.

382. *See* Clark, *supra* note 252, at 326 (2010) (quoting OFFICE OF MGMT. & BUDGET, *supra* note 252, at 2) (internal quotation marks omitted).

383. OFFICE OF MGMT. & BUDGET, *supra* note 252, at 2.

protections and have fewer ways to report misconduct than other types of whistleblowers. The distinction President Obama and the law make among whistleblowers is based on the separation of powers tension between oversight and transparency on the one hand and secrecy on the other. Congress wants to encourage employees to disclose governmental misconduct related to national security, while Presidents want to keep vital national security information secret, even from Congress. National security whistleblowers are caught in this crossfire.

IV. PROVIDING A BETTER BALANCE

> The contradictions and tensions of secrecy are never stronger than in the military stance of nations.
>
> *Sissela Bok (1982)*[384]

The answer to the second question I posed at the beginning of the Article – does Obama's distinction make sense? – depends on how one views the inevitable tradeoff society must make between secrecy and transparency in government. As Steven Aftergood, a prominent researcher on secrecy policy for the Federation of American Scientists, asserted, Americans "seem to be of two minds about secrecy."[385] On the one hand, a democracy abhors secrecy – to govern ourselves and hold elected leaders accountable, we must have access to information.[386] On the other hand, government needs some secrecy to function well.[387] For example, the Supreme Court concluded that some confidentiality assists a President in receiving good advice from advisors, and the importance of such secrecy "is too plain to require further discussion."[388] The Court went so far as to say that this confidentiality privilege for the Chief Executive "is fundamental to the operation of Government, and inextricably rooted in the separation of powers under the Constitution."[389] Others have noted the "ever-delicate balance"

384. *Cf*. BOK, *supra* note 12, at 191.

385. Steven Aftergood, *National Security Secrecy: How the Limits Change*, 77 SOC. RES. 839, 839 (2010).

386. *See id*. at 839; *see also* Halperin & Hoffman, *supra* note 259, at 132 ("The public's 'right to know' has always been a basic tenet of American political theory.").

387. *See* BOK, *supra* note 12, at 174 ("[G]overnment secrecy is not always an evil. Among the many kinds of information that modern governments obtain, store, and generate, there are some that nearly all would agree to protect from full publicity [such as] personnel files . . . tentative drafts circulated for discussion within an agency . . . or sensitive explorations of changes in monetary policy . . . ").

388. United States v. Nixon, 418 U.S. 683, 705 (1974); *see also id*. ("Human experience teaches that those who expect public dissemination of their remarks may well temper candor with a concern for appearances and for their own interests to the detriment of the decisionmaking process.").

389. *Id*. at 708.

between transparency and secrecy,[390] for as Professor Heidi Kitrosser observed, "[i]t is hardly news that secrecy has costs and benefits."[391]

Society seems particularly willing to accept secrecy when it relates to national security. Aftergood asserted that "there is a near universal consensus that some measure of secrecy is justified and necessary to protect authorized national security activities, such as intelligence gathering and military operations."[392] Sissela Bok, a noted secrecy scholar, concluded that "every state requires a measure of secrecy in order to defend itself against enemy forces. The legitimacy of such secrecy in self-defense is clear-cut."[393]

Indeed, in *United States v. Nixon*,[394] although the Supreme Court determined that a President must respond to a subpoena in a criminal case requesting generalized information, the Court indicated the executive confidentiality privilege might require a different result if the issue related to military or diplomatic secrets.[395] In a separate case, the Court upheld a state secrets privilege that permitted the executive branch to refuse to provide information in a case after showing that "compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged."[396] Professor Kitrosser noted that secrecy's costs and benefits become amplified in the national security context because "they often consist not only of competing values (e.g., democratic openness versus national security) but also of competing means of achieving the same value (e.g., national security through openness versus national security through secrecy)."[397]

Yet, even in this context, too much secrecy can occur. Bok argued that

390. Sulmasy, *supra* note 253, at 1229.

391. *See* Kitrosser, *supra* note 252, at 1064; *see generally* BOK, *supra* note 12.

392. *See* Aftergood, *supra* note 385, at 839; *see also* Ryan M. Check & Afsheen John Radsan, *One Lantern in the Darkest Night: The CIA's Inspector General*, 4 J. NAT'L SEC. L. & POL'Y 247, 247 (2010) ("Gathering intelligence and conducting covert action, by their nature, depend on secrecy."); Sulmasy, *supra* note 253, at 1232 ("An acceptance of greater government secrecy is a tacit part of the decision making when any democratic nation commits to engage in armed conflict.").

393. BOK, *supra* note 12, at 191. Bok also recognized several problems with military secrecy, arguing that "secrecy is as often a weapon in the hands of the aggressors and an aid in every scheme of oppression." *Id*.

394. 418 U.S. 683 (1974).

395. *See id*. at 710 (noting this distinction and asserting that "courts have traditionally shown the utmost deference to Presidential responsibilities"). The Court hinted that if the information related to "military, diplomatic, or sensitive national security secrets," it might not even require the President to produce the information for a court's *in camera* review. *See id*. at 706.

396. United States v. Reynolds, 345 U.S. 1, 10 (1953).

397. Kitrosser, *supra* note 252, at 1064; *see also* Erwin Chemerinsky, *Panel: Secrecy and Barriers to Open Government*, 57 AM. U. L. REV. 1234, 1238 (2008) ("The need for Executive Branch secrecy is greatest when foreign policy and national security issues are implicated.").

many levels of secrecy undermined the failed helicopter rescue of the hostages in Iran in 1980, including keeping the final decision secret from those in the Carter Administration who thought it was too risky to proceed.[398] Thus, "secrecy directed against military opponents can also come to distort domestic choices . . . [and] can cause reasoning and planning to go astray."[399] More recently, the 9/11 Commission blamed excessive secrecy for leaving the country vulnerable to attack, because various government agencies' insistence on secrecy led to a lack of inter-agency communication.[400] Secrecy, even in the intelligence community, can undermine accountability,[401] particularly the executive branch's accountability to the legislative and judicial branches. Ultimately, for example, Professor Kitrosser argued for more transparency and less secrecy, noting that "national security based secrecy needs are dramatically overstated" and that secrecy encourages "poorly informed and under-vetted decision-making."[402]

Inevitably, this balancing becomes context-specific. Everyone likely understands the absolute necessity to have kept secret the operation that found Osama bin Laden in May 2011 in order to catch him by surprise.[403] But, fewer people would support classifying documents to hide illegal or embarrassing conduct, particularly if the conduct has only a tangential relationship to national security.[404] Interestingly, whistleblowing in the national security context squarely presents the issue of how best to balance our desire for transparency with our need for secrecy.

A. The National Security Whistleblowing Dilemma

An intelligence community employee who leaked information about the bin Laden operation ahead of time would rightly face severe public criticism and likely criminal prosecution, while the same employee blowing the whistle on government corruption in the FBI might receive societal praise.[405] But, examples in the middle of these extremes present problems.

398. *See* BOK, *supra* note 12, at 195-96.

399. *Id*. at 196.

400. *See* NAT'L COMM'N ON TERRORIST ATTACKS ON THE U.S., THE 9/11 COMMISSION REPORT 417 (2004) ("Current security requirements nurture overclassification and excessive compartmentation of information among agencies.").

401. Check & Radsan, *supra* note 392, at 247.

402. Kitrosser, *supra* note 252, at 1066.

403. *See, e.g.*, Mark Mazzetti et. al., *Behind the Hunt for Bin Laden*, N.Y. TIMES, May 3, 2011, at A1.

404. *Cf*. Exec. Order No. 13,526, § 1.7, 75 Fed. Reg. 707 (Jan. 5, 2010) (prohibiting the classification of information as secret in order to "prevent embarrassment" or to "prevent or delay the release of information that does not require protection in the interest of the national security").

405. The Deep Throat source for the revelations about Nixon and the Watergate scandal may be a good example of this latter proposition. *See generally* CARL BERNSTEIN & BOB WOODWARD, ALL THE

What about the whistleblower who exposes a government program that is illegal but also one that effectively protects national security? Or one who publicizes wasteful military spending, but also discloses important military intelligence in the process? Answering how best to balance secrecy and transparency to encourage the right type of whistleblowing but to discourage leaks harmful to national security becomes extremely difficult.[406]

In many ways, good reasons exist to support Obama's distinction and treat disclosures related to national security information differently than other types of disclosures. Just as the issue of national security might make us willing to accept a higher level of governmental secrecy, even a whistleblower advocate might also be willing to accept more limited antiretaliation protection for government employees who reveal national security information. The easiest cases would involve leaks of classified information that have little to do with government misconduct. Some might not consider such leakers to be "whistleblowers" deserving protection because, as a definitional matter, a whistleblower believes he or she is revealing illegal, unethical, or improper misconduct in the public interest.[407] For example, the 1998 revelation in the media that the U.S. was tracking Osama bin Laden's satellite phone arguably caused bin Laden to stop using the phone, which of course made him harder to follow and did not reveal any governmental misconduct.[408] Similarly, the U.S. classified documents revealed to WikiLeaks provide some embarrassing and often scandalous information, but they revealed arguably little in the way of illegal government conduct.[409] For example, the State Department cables released by WikiLeaks revealed

PRESIDENT'S MEN (1974); *see also* Susan Page & Mark Memmott, *"Deep Throat" Was Ultimate Whistleblower to Some*, USA TODAY, May 31, 2005, at 4A (noting that, although some criticized Mark Felt, who was revealed as Deep Throat, others considered him to be the "ultimate whistleblower, a man who saw wrongdoing and exposed it at risk to his own career"), *available at* <http://www.usatoday.com/news/washington/2005-05-31-deep-throat-inside_x.htm>. Notably, TIME magazine named an FBI whistleblower, Colleen Rowley, a "Person of the Year," for trying to reveal government bumbling before 9/11. *See* Richard Lacayo & Amanda Ripley, *Persons of the Year*, TIME, Dec. 30, 2002, at 31.

406. *Cf*. BOK, *supra* note 12, at 202 (concluding that the question of whether "informed debate and government accountability" can survive in the national security context to be "the most difficult of all those that secrecy raises").

407. *See* Randy Borum et al., *The Psychology of "Leaking" Sensitive Information: Implication for Homeland Security*, 1 HOMELAND SEC. REV. 97, 97 (2006); Janet P. Near & Marcia P. Miceli, *Organizational Dissidence: The Case of Whistle-Blowing*, 4 J. BUS. ETHICS 1, 4 (1985) (defining whistleblowing as involving the reporting of "illegal, immoral, or illegitimate" behavior).

408. *See* Porter Goss, *Loose Lips Sink Spies*, N.Y. TIMES, Feb. 10, 2006, at A25 ("The [bin Laden disclosure] was, without question, one of the most egregious examples of an unauthorized criminal disclosure of classified national defense information in recent years. It served no public interest.").

409. *See* Ginger Thompson, *Competing Portraits in WikiLeaks Case*, N.Y. TIMES, Dec. 23, 2011, at A15 (noting that Manning's lawyers argued in court that none of the leaked information damaged national security). *But see infra* text accompanying notes 425-26 (describing some arguably illegal conduct).

that Muammar Gaddafi enjoyed the company of "four blond Ukrainian nurses" and that a U.S. diplomat called North Korea's former President Kim Jong Il "flabby."[410]

Although serving no interest other than being "anti-secrecy," disclosures like these could damage diplomatic relationships and undermine U.S. government initiatives internationally. In addition to petty disclosures, the State Department cables published by WikiLeaks revealed that Arab countries have requested that the U.S. attack Iran's nuclear facilities, even though those countries publicly promote their relationship with Iran.[411] These cables did not reveal any U.S. misconduct and could be damaging because they disclosed behind-the-scenes communications that differ from some countries' public stances.[412] Secretary of State Hilary Clinton stated that publishing the WikiLeaks' cables "puts people's lives in danger, threatens national security and undermines our efforts to work with other countries to solve shared problems."[413] Such leaks may make the government more transparent, but they hurt national security without serving any other public interest, such as exposing misconduct.

Yet, even when whistleblowers reveal purported wrongdoing, treating national security whistleblowing differently than other types of whistleblowing may make sense as well. National security whistleblowers might disclose damaging information and be wrong about its illegality because national security issues often present nuanced and complicated problems.[414] For example, a Department of Defense employee could release classified information to a reporter about military action he incorrectly believed to be illegal, endangering people's lives and exposing weaknesses that could be exploited by our enemies. Such disclosures cause greater harm than the typical whistleblower disclosure related to financial matters or mismanagement, without create any offsetting public good by revealing any actual

410. *See* Massimo Calabresi, *The War on Secrecy*, TIME, Dec. 13, 2010, at 30, *available at* <http://www.time.com/time/magazine/article/0,9171,2034488,00.html>.

411. *See id*.

412. *Cf*. Snepp v. United States, 444 U.S. 507, 512 (1980) (noting that revealing even unclassified information can harm national interests because "[i]n addition to receiving intelligence from domestically based or controlled sources, the CIA obtains information from the intelligence services of friendly nations and from agents operating in foreign countries. The continued availability of these foreign sources depends upon the CIA's ability to guarantee the security of information that might compromise them and even endanger the personal safety of foreign agents").

413. Calabresi, *supra* note 410. By contrast, Defense Secretary Robert Gates stated, "Is this embarrassing? Yes. Is it awkward? Yes. Consequences for U.S. foreign policy? I think fairly modest." *Id*.; *see also* Thompson, *supra* note 409 (noting that Manning's lawyers argued in court that none of the leaked information damaged national security).

414. *Cf*. Richard J. Barnet, *The Ideology of the National Security State*, 26 MASS. REV. 483, 495 (1985) (noting that the topic of national security is "amorphous and seemingly complex"), *quoted in* Heidi Kitrosser, *What If Daniel Ellsberg Hadn't Bothered?*, 45 IND. L. REV. 89, 95 (2011).

misconduct.[415]

This ambiguity may be compounded because the dangers of the disclosure and the legality of conduct disclosed may not be clear when the information is disclosed. As discussed above, Jeffrey Sterling allegedly told James Risen about government waste and mismanagement in an intelligence program focused on Iran.[416] The government asserted that Sterling's alleged leak involved the disclosure of a human asset, which "placed at risk our national security and the life of an individual working on a classified mission," according to Assistant Attorney General Lanny A. Breuer.[417] On the other hand, Sterling's defenders argue that it involved information about an out-of-date botched undercover mission that did nothing damaging except embarrass the government.[418] In fact, by the time Risen published the book that included information allegedly from Sterling, the government was shutting down the program as a failure costing almost $100 million.[419] It may be hard to judge whether and how much a leak damaged national security, even years after a leak. Protecting whistleblowers in such ambiguous circumstances may result in too many disclosures of secrets without enough exposure of wrongdoing.

Finally, assuming the employee was right about conduct being illegal, he or she might not understand the larger context for certain government conduct. As the Supreme Court found in a related context in *Snepp v. United States*,[420] "When a former agent relies on his own judgment about what information is detrimental, he may reveal information that the CIA – with its broader understanding of what may expose classified information and confidential sources – could have identified as harmful."[421]

Another example relates to what some have called the "mosaic theory" to support a "state secrets" executive privilege: intelligence may seem innocuous by itself, but will become more important when combined with

415. *See generally* Lee, *supra* note 170, at 1466 n.62 (noting numerous government assertions that leaks caused significant damage to national security); *cf.* Check & Radsan, *supra* note 392, at 251-52 ("[W]hen the USDA operates ineffective programs or violates the law, the scandals are likely to be contained within the borders of our country and the losses confined to the national treasury. By contrast, when the CIA faces problems, they are likely to implicate our national security, to affect our relations with other countries, and to put lives at risk.").

416. *See supra* text accompanying notes 218-23.

417. Thomas et al., *supra* note 166.

418. *See* Greenwald, *supra* note 220 ("While there is no good faith claim that Risen's revelation six years after the fact harmed U.S. national security, Risen's story was unquestionably newsworthy because it revealed how inept and ignorant American intelligence agencies are when it comes to Iran.").

419. *See* Harris, *supra* note 226.

420. 444 U.S. 507 (1980). In *Snepp*, the Court found that the CIA could enforce an agreement with a former employee permitting the CIA to review any of the employee's writings prior to publication, even if the writings did not reveal classified information. *See id*. at 512-16.

421. *Id*. at 512.

other seemingly unimportant bits of information.[422] A whistleblower's inability or unwillingness to see the big picture may lead to the harmful disclosure of national security information. For example, the *New York Times* published WikiLeaks' Guantanamo files on the internet one week before the raid that killed Osama bin Laden. These files included a document from which bin Laden could have inferred that the U.S. had learned the identity of bin Laden's courier (and thus possibly where bin Laden was hiding), meaning that "the house [where bin Laden was killed] could have been empty when the SEALs arrived."[423] Like the Supreme Court in *Snepp*, we might question whether a potential whistleblower should be the person balancing the benefits of revealing the illegality against the costs to our national security from its disclosure.

Yet, exposing illegality, government waste, gross mismanagement, and abuse of authority is just as important in the national security context as in other contexts – if not more so. The whistleblowers who exposed the Bush Administration's domestic wire-tapping, secret CIA renditions, and waterboarding torture methods revealed important information about arguably illegal activities and also allowed public debate about the way in which the country fought the war on terror.[424] Further, although WikiLeaks published numerous classified documents revealing little in the way of illegality, the website also published a disturbing video about an apparently illegal attack on Afghanistan civilians by a U.S. Army helicopter.[425] One commentator asserted that

> many of WikiLeaks' disclosures over the last 18 months have directly involved improprieties, bad acts and even illegalities on the part of [Secretary of State Hillary] Clinton's own State Department. As part of WikiLeaks' disclosures, she was caught ordering her diplomats at the U.N. to engage in extensive espionage on other diplomats and U.N. officials; in a classified memo, she demanded "forensic technical details about the communications systems used by top UN officials, including passwords and personal encryption keys used in private and commercial networks for official communications" as well as "credit card numbers, email addresses, phone, fax and pager numbers and even frequent-flyer account numbers" for a whole slew of diplomats, actions previously condemned

422. *See* SCHOENFELD, *supra* note 249, at 213; Christina E. Wells, *State Secrets and Executive Accountability*, 26 CONST. COMMENT. 625, 635 (2010).

423. Graham Allison, *The Biggest Bet*, TIME, May 7, 2012, at 34, 40.

424. *See* Kitrosser, *supra* note 252, at 1052 (discussing arguments regarding legality of wiretapping); *see also* Isikoff, *supra* note 239 (discussing legality of NSA wiretaps); Shane, *WikiSafe*, *supra* note 151, at WK1 ("All those disclosures led to public debate and to action: the prisons were closed; coercive interrogations were banned; the N.S.A. program was brought under court supervision.").

425. *See* Shane, *supra* note 132 (stating that Manning was "suspected of passing a classified video of an American military helicopter shooting Baghdad civilians").

by the U.S. as illegal.[426]

The law should not permit illegal conduct to hide behind a veil of secrecy, even in the name of national security.

Additionally, just because a government official labels information as "classified" does not mean it *should* be classified. The government systematically over-classifies documents as "secret."[427] For example, in 2010, the federal government classified almost 77 million documents, a 40 percent increase over the previous year.[428] (Government officials state this increase was due, at least in part, to better reporting by officials.)[429] Steven Aftergood, the scholar on government transparency mentioned earlier, provided a terrific example of the often-incoherent nature of government classification: as of 2002, the government declassified the 1997 and 1998 budgets for CIA intelligence, but kept the budget total from 1947 classified.[430] Journalists and others have argued that government officials "use classification to hide embarrassing information about wrongdoing."[431] Some whistleblowers, like Daniel Ellsberg perhaps, simply act in "the public interest by exposing important, wrongly classified information." [432]

The government also can exaggerate the harm that comes from reveal-

426. Glenn Greenwald, *Hilary Clinton and Internet Freedom*, SALON (Dec. 9, 2011, 2:40 AM CDT), <http://www.salon.com/2011/12/09/hillary_clinton_and_internet_freedom/singleton/>; *see also* Glenn Greenwald, *What WikiLeaks Revealed to the World in 2010*, SALON (Dec. 24, 2010, 4:25 AM CDT), <http://www.salon.com/2010/12/24/wikileaks_23/> (providing links to newspaper stories about WikiLeaks revelations concerning U.S. government misconduct).

427. *See* BOK, *supra* note 12, at 197 ("Mountains of worthless information are stamped Top Secret; levels of secrecy multiply."); Steven Aftergood, *On Leaks of National Security Secrets: A Response to Michael Hurt*, 8 NAT'L SEC. STUD. Q. 97, 97 (2002) ("A considerable quantity of information that is not sensitive is nevertheless formally classified."); William H. Freivogel, *Publishing National Security Secrets: The Case for "Benign Indeterminacy,"* 3 J. NAT'L SEC. L. & POL'Y 95, 99 (2009) ("[T]he government engages in a vast amount of overclassification, which hid damaging information about the mishandling of the Vietnam War and about extensive tapping of telephone conversations without warrants."); Kitrosser, *supra* note 170, at 894 ("There long has been widespread concern across the political spectrum about the existence of rampant overclassification.").

428. *See* Scott Shane, *Complaint Seeks Punishment for Classification of Documents*, N.Y. TIMES, Aug. 2, 2011, at A16.

429. *See id*.

430. *See* Aftergood, *supra* note 427, at 98 (calling such inconsistencies "capricious[]").

431. Freivogel, *supra* note 427, at 98. Similarly, Daniel Ellsberg has argued,

> [T]he apparatus of secrecy serves in very significant part to conceal – from American voters, Congress, courts – policy errors, recklessness, violation of domestic and international law, deception, crimes, corruption in various forms, questionable or disastrous judgment, responsibility for catastrophes. The motivations for classifying these are real and strong, not just a reflection of carelessness. But they have to do with considerations of domestic and bureaucratic politics and blame avoidance, not at all with true national security.

Ellsberg, *supra* note 243, at 797; *see also* BOK, *supra* note 12, at 198 ("[T]he appeal to 'national security' offers a handy reason to avoid scrutiny of neglect, mistakes, and abuses.").

432. *See* Kitrosser, *supra* note 414, at 118.

ing classified information.[433] For example, in the Pentagon Papers case, the government claimed that eleven specific secrets the papers revealed would harm peace talks and prolong the Vietnam War if the *New York Times* published them.[434] Later, however, Solicitor General Erwin Griswold admitted that he has "never seen any trace of a threat to the national security from the publication" of the secrets.[435] Similarly, although President Bush claimed that the *New York Times* would have "blood on their hands" if it published the domestic wiretapping story, many have noted that the government has never demonstrated any proof that the publication resulted in damage to national security.[436]

Sometimes national security whistleblowers reveal *un*classified information, but it relates to national security and thus raises the government's sensitivities. Thomas Drake and others on his behalf asserted that he did not reveal anything related to national security secrets; rather, he exposed government waste and mismanagement.[437] Similarly, Franz Gayl revealed bureaucratic self-dealing and ineptitude that kept soldiers in Iraq from receiving specially armored vehicles.[438] The Marines, however, revoked his security clearance for relatively innocuous references in a public report about two internal requests for equipment that he made while stationed in Iraq.[439]

In short, society's expectations regarding the relative importance of

433. *See* Freivogel, *supra* note 427, at 95-96 ("White House and other national security officials routinely exaggerate the dangers of publishing secret information. Over the decades, government officials have presented scant proof of harm from such activities."); Wells, *supra* note 422, at 635 (noting that the "government's tendency to exaggerate national security harms posed by the release of information is well-documented").

434. *See* Freivogel, *supra* note 427, at 112 (describing secrets). As Professor Freivogel noted,

> These eleven secrets considered to be the most dangerous items within the Pentagon Papers volumes involve sensitive subjects in which the government has a strong interest – diplomatic initiatives, intelligence activities, intelligence estimates and capabilities, and military contingency plans. The government claimed that disclosure of the Pentagon Papers could endanger the lives of intelligence agents and prolong the war, with the resulting death of thousands more soldiers and many prisoners of war.

See id. at 113.

435. Erwin N. Griswold, *Secrets Not Worth Keeping: The Courts and Classified Information*, WASH. POST, Feb. 15, 1989, at A25, *quoted in* Freivogel, *supra* note 427, at 113. An expert at Daniel Ellsberg's trial buttressed this claim by asserting that "at most" 5 percent of the classified material Ellsberg disclosed actually had potential relevance to national security when it originated, and that ½ to 1 percent still had sufficient relevance to justify secrecy protection after two or three years. *See* Ellsberg, *supra* note 243, at 794.

436. *See* Freivogel, *supra* note 427, at 113.

437. *See* Mayer, *supra* note 7, at 55; Greenwald, *supra* note 144 ("Drake's leak involved no conceivable harm to national security, but did expose serious waste, corruption and possible illegality.").

438. *See* James Verini, *The Unquiet Life of Franz Gayl*, THE WASH. MONTHLY, Aug. 2011, at 21, *available at* <http://www.washingtonmonthly.com/magazine/julyaugust_2011/features/the_unquiet_life_of_franz_gayl030495.php?page=all&print=true>.

439. *See id*.

secrecy or transparency for national security whistleblowers may vary depending on the situation. At times it makes sense to treat national security whistleblowers less protectively than other types of whistleblowers, but at other times we may want to provide more encouragement to them. Developing general rules and legal incentives in this environment can be challenging because the factual circumstances involved vary from case to case.

In Part III, I concluded that the law as it stands now prefers transparency over secrecy for most types of whistleblowers. However, in the face of these factual uncertainties and given the potential devastating consequences for national security, the law has broadly protected secrecy at the cost of transparency and oversight with regard to national security whistleblowers. Reforming the current system to provide more protection for national security whistleblowers in order to increase transparency could undermine our legitimate need for secrecy in some contexts. Yet, this conclusion assumes that we exist in a "zero-sum" world, in which transparency gains only if secrecy loses, and vice versa. In the next section, I question this assumption and explore whether changes to the law affecting national security whistleblowers might alter the scale to provide for more transparency, but without negatively affecting secrecy.

B. Suggestions for Reform

Commentators have identified several different models the law utilizes to encourage whistleblowers.[440] Currently, the law affecting national security whistleblowers uses three of them – structural disclosure channels, antiretaliation protection, and imposing a duty to blow the whistle – but they have flaws as applied in this context. Indeed, as I discussed above, Congress contemplated revising the law addressing national security whistleblowers during the last several sessions, but could not reach an agreement.[441] In this section, I broadly outline some considerations about each of these models that may inform congressional debate going forward, with the goal of increasing governmental transparency without sacrificing necessary

440. *See* Yuval Feldman & Orly Lobel, *The Incentives Matrix: The Comparative Effectiveness of Rewards, Liabilities, Duties, and Protections for Reporting Illegality*, 88 TEX. L. REV. 1151, 1154 (2010) (discussing "four prototypical legal mechanisms designed to promote individual reporting: (1) Antiretaliation Protection; (2) Duty to Report; (3) Liability Fines; and (4) Monetary Incentives"); Richard Moberly, *Protecting Whistleblowers by Contract*, 79 COLO. L. REV. 975, 995 (2008) (concluding that some whistleblowers may be protected by an employer's contractual promise not to retaliate); Richard E. Moberly, *Sarbanes-Oxley's Structural Model to Encourage Corporate Whistleblowers*, 2006 B.Y.U. L. REV. 1107, 1132 (identifying a "structural model" in which employees may utilize a disclosure channel to report misconduct) [hereinafter Moberly, *Structural Model*].

441. *See supra* text accompanying notes 190-217.

secrecy.[442]

1. Enhanced Disclosure Channels

When balancing transparency and secrecy, we should be clear about where those terms are directed: Transparent to whom? Secret from whom? Transparency can mean making government decisions more transparent to the *public*, which we generally desire but which becomes problematic when juxtaposed against the need for secrecy regarding national security. However, we could attain transparency for national security by making executive branch decisions transparent to *Congress*. Such transparency assists legislative oversight, another important value balanced against secrecy. In other words, the need for secrecy in national security affairs might generally trump transparency to the public. However, secrecy should give way to transparency to Congress because of its constitutional responsibility as a check on the executive branch.[443]

Problems in the national security context can become more transparent to Congress through the use of structural disclosure channels for whistleblowers to report misconduct directly to Congress if the executive branch does not address it. Currently, various laws provide national security whistleblowers ways to disclose wrongdoing internally to an IG, who is located within the executive branch itself.[444] However, Congress will find out about the report only in certain circumstances: (1) through a semi-annual report the IG sends to the agency head, who must pass it on to Congress;[445] (2) if the IG becomes aware of "particularly serious or flagrant problems, abuses, or deficiencies," and makes a report to the agency head who must send it to Congress;[446] or (3) in response from a demand to report to Congress an "urgent concern," if the head of an agency permits a whistleblower to talk

442. I should note that at least one commentator, Professor Stephen Vladeck, believes that the current system works well in the "vast majority of cases." Vladeck, *supra* note 296, at 1544. However, Vladeck notes that the system does not work well when the highest levels of government appear to approve misconduct. *See id*. at 1544-46 (noting that in these cases "the likelihood that disclosure pursuant to the WPA or the ICWAP (to the extent they apply) will actually allow for meaningful oversight of the program is fleeting, at best"). Vladeck astutely points out that, paradoxically, these are "the cases where whistleblowing is the *most* important – where government employees are involved in an illegal program that has approval from the most senior officials in the relevant agencies and departments." *Id*. at 1544.

443. *See* Kitrosser, *supra* note 250, at 522-27; Kitrosser, *supra* note 170, at 916-18.

444. *See, e.g.*, 50 U.S.C. § 403q (2006) (CIA IG). The Civil Service Reform Act does assert that employees have a "right" to give information to Congress. *See* 5 U.S.C. § 7211 (2006). However, that right does not attach to a remedy. The WPA provides remedies for prohibited personnel practices like retaliation, but the WPA does not apply to most members of the intelligence community. *See id*. §§ 2302(a)(1) & (2)(C).

445. *See, e.g.*, 50 U.S.C. § 403q(d)(1) (CIA IG).

446. *See, e.g.*, *id*. § 403q(d)(2) (CIA IG).

with Congress.[447] In other words, the law allows for an agency head or IG to filter, and even block, reports to Congress from national security whistleblowers.[448]

Although IGs theoretically provide an independent investigation of whistleblower reports, the President may remove an IG,[449] and IGs typically act under the supervision of an agency head. As an example, the CIA's IG reports directly to and is "under the general supervision" of the Director of the CIA.[450] Moreover, the Director can prohibit the IG from conducting an investigation into wrongdoing if the Director determines the prohibition "is necessary to protect vital national security interests."[451] The Director must report this type of order to Congressional intelligence committees,[452] but, again, Congress only receives secondary and filtered information about the disclosure.

The new IG position for the entire intelligence community, described above,[453] resolves some of the inherent tensions of an IG investigating the IG's own agency because it would permit an investigation from someone outside of a specific agency. But, the law subjects this overarching IG to restrictions similar to those of other IGs, including control by the Director of National Intelligence.[454] The Director in charge of intelligence will still control all of the investigation and reporting to Congress. An IG may be a good first option to receive whistleblower disclosures, but the IG cannot be the *only* option because an IG is inherently an internal (rather than external) check subject to the ultimate control of the executive branch.[455] For example, IGs from intelligence agencies offered little assistance during the warrantless surveillance controversy because they did not offer a view on the legality of the program, could not compel testimony, and did not receive

447. *See, e.g.*, *id*. § 403q(d)(5) (CIA IG).

448. *See* Moberly, *Structural Model*, *supra* note 440, at 1121-24 (describing blocking and filtering problems with whistleblower reports).

449. *See, e.g.*, 50 U.S.C. § 403q(b)(6) (CIA IG). If a President removes the IG, the President must provide the reasons for the removal to Congressional intelligence committees. *See id*.

450. *See id*. § 403q(b)(2).

451. *Id*. § 403q(b)(3).

452. *See id*. § 403q(b)(4); 50 U.S.C. § 403-3h(f)(2) (2006).

453. *See supra* text accompanying notes 353-70.

454. *See* 50 U.S.C. §§ 403-3h(k); 403-3h(c); 403-3h(f).

455. *See* Sarah Wood Borak, *The Legacy of "Deep Throat": The Disclosure Process of the Whistleblower Protection Act Amendments of 1994 and the No FEAR Act of 2002,* 59 U. MIAMI L. REV. 617, 640 (2005) (noting that IGs are theoretically independent but they are placed in the agencies themselves and "lack both decision-making and enforcement powers, which limits the overall effectiveness of the disclosure process"); Kitrosser, *supra* note 271, at 511. Assuming this remains the only option, Check and Radsan make a thoughtful suggestion that an IG's term could straddle presidencies, like the Director of the FBI who is appointed for a ten-year term, thus reducing presidential influence. *See* Check & Radsan, *supra* note 392, at 292.

support from key members of the Bush Administration.[456] In other cases, such as with CIA renditions and the "enhanced interrogation techniques" used against terror suspects, the press found out about the problems before the CIA IG.[457] Two commentators explained these events by arguing that the IG's "reputation within the Agency is so low that people risk prosecution [by leaking to the press] rather than merely report their concerns to the authorized internal guard."[458] As a result, according to some, "[a]gency Inspectors General have proven themselves ineffective defenders of whistleblower rights," suggesting that Congress require more information on IG investigations to permit enhanced legislative oversight.[459] Indeed, some have argued that during the 1990s and 2000s, congressional oversight of national security issues became "dysfunctional"[460] and "broken"[461] in part because excessive executive branch secrecy kept the right information from getting to Congress.[462]

Whistleblowers can help with that information flow if their information has a more direct route to individuals who can truly investigate complaints should the IG route prove insufficient.[463] Congress needs direct, unfiltered reports from national security whistleblowers if the executive branch does not resolve problems identified by whistleblowers. Some may object to providing a direct line to Congress for fear that it would compromise necessary secrecy regarding national security matters. However, congressional members have relevant security clearances, as do many members of their staff.[464] As important, both the House and Senate have in place procedures to handle classified information.[465] The Security Act of 1947

456. *See* Kitrosser, *supra* note 271, at 511.

457. *See* Check & Radsan, *supra* note 392, at 288.

458. *Id*.

459. *See* GOODMAN ET AL., *supra* note 187, at 21. Not everyone agrees. Check and Radsan assert that "[t]he [CIA] IG, straddled between two branches, has enough independence to do the job." Check & Radsan, *supra* note 392, at 292.

460. NAT'L COMM'N ON TERRORIST ATTACKS ON THE U.S., *supra* note 400, at 420 ("Congressional oversight for intelligence – and counterterrorism – is now dysfunctional.").

461. DENIS MCDONOUGH ET AL., CTR. FOR AM. PROGRESS, NO MERE OVERSIGHT: CONGRESSIONAL OVERSIGHT OF INTELLIGENCE IS BROKEN 15 (2006).

462. *See id*. at 27 ("First and foremost, of course, is that much of intelligence agency work takes place under the shroud of extreme secrecy. Congressional overseers – members and staff alike – do not know what they do not know."); Kitrosser, *supra* note 252, at 1058-59 (detailing problems with oversight even when Congress receives classified briefings).

463. *See* Moberly, *Structural Model*, *supra* note 440, at 1149-50 (describing the benefits of Sarbanes-Oxley's requirement that corporations install a whistleblower disclosure channel permitting employees to report misconduct directly to the audit committee of the board of directors, which would bypass management blocking and filtering).

464. *See* Kitrosser, *supra* note 252, at 1073-74, 1077.

465. *See id*. at 1073-75, 1080-84 (describing Congressional rules for handling classified information).

already contemplates that Congress, through its intelligence committees or the "Gang of Eight," should receive information about intelligence activities and covert operations.[466] Thus, if the law directed whistleblowers to authorized people in Congress with a procedure set up to handle classified information, then whistleblowers could assist with transparency about national security without a corresponding decrease in secrecy.[467] The transparency would not be to the public generally, but it would be to a separate branch of government constitutionally charged with oversight of the executive branch.[468]

Accepted theory regarding whistleblower disclosure channels also supports permitting reports to Congress. Professor Wim Vandekerckhove has set forth a "three tiered" model for disclosure, in which a whistleblower should first report internally within an organization.[469] The whistleblower should report externally only if the internal disclosure does not address the misconduct successfully.[470] If so, the next "tier" of disclosure would be to a regulator, "acting on behalf of wider society."[471] Congress serves perfectly as the outside regulator to the executive branch because of its oversight obligations and because, to use Vandekerckhove's words, Congress has "a controlling mandate with regard to [the executive branch], derived directly or indirectly from a political representation of society."[472] I discuss whether national security whistleblowers should be permitted to disclose to a third tier – the general public – in the final section of this Part.[473]

A second objection to permitting executive branch whistleblowers greater access to Congress, which is more difficult to resolve definitively, involves the current separation of powers détente described in Part III. The issue here is not as much about secrecy as about Presidential power to determine if, when, and how the executive branch will give information about national security to the legislative branch. The President's constitutional

466. *See* 50 U.S.C. § 413(a)(1) (2006) (noting that the executive branch must keep the "congressional intelligence committees . . . fully and currently informed of the intelligence activities of the United States, including any significant anticipated intelligence activity"); *id.* § 413b (providing procedures for informing Congress about covert actions).

467. *See* Kitrosser, *supra* note 252, at 1075 ("Congress is considered to have a reliable track record for non-leakage and it has a political incentive to avoid leaks in order to avoid blame by the executive branch for the same.").

468. *Cf.* BOK, *supra* note 12, at 110 ("Even where persuasive reasons for collective practices of secrecy can be stated, accountability is indispensible.").

469. *See* Wim Vandekerckhove, *European Whistleblower Protection: Tiers or Tears?*, *in* A GLOBAL APPROACH TO PUBLIC INTEREST DISCLOSURE: WHAT CAN WE LEARN FROM EXISTING WHISTLEBLOWING LEGISLATION AND RESEARCH? 15, 18 (David Lewis ed., 2010).

470. *See id.*

471. *See id.*

472. *Id.*

473. *See* discussion *infra* Part IV.B.iv.

prerogatives for secrecy are at their height when national security is at stake. Although Congress has never accepted that the President's power in this field is exclusive, Congress also has not shown a willingness to challenge such arguments.[474]

It should. First, as a statutory matter, one hundred years ago, Congress gave a "right" to federal employees to give information to Congress, a right currently located in the Civil Service Reform Act that applies to *all* employees – without an exception for intelligence community workers.[475] Supporting that right with statutorily-mandated disclosure channels would seem to fall easily within the power of Congress. Second, as a constitutional matter, Congress has a constitutional role in protecting national security. Professor Kitrosser argued persuasively that the Constitution envisions a "robust structural checking" by Congress of Presidential power, in which "the executive branch can be given vast leeway to operate in secret, but remains subject to being overseen or otherwise restrained in its secrecy by the legislature."[476] Allowing Congress to limit Presidential secrecy permits the balancing between constitutional norms of secrecy and transparency required by national security whistleblowers:

> On the one hand, the Constitution clearly values transparency as an operative norm. This is evidenced by myriad factors, including the necessities of self-government, the First Amendment, and Article I's detailed requirements for a relatively open and dialogic legislative process. On the other hand, the Constitution reflects an understanding that secrecy sometimes is a necessary evil, evidenced both by the congressional secrecy allowance [in Article I, section 5, clause 3] and by the President's structural secrecy capabilities. Permitting executive branch secrecy, but requiring it to operate within legislative parameters, themselves open and subject to revision, largely reconciles these two values.[477]

Louis Fisher, who testified before Congress on this issue, made a similar argument that "Congress has coequal duties and responsibilities for the

474. *See, e.g.* S. REP. NO. 111-101, at 27 (2009) (noting that in the debate over the ICWPA, Congress agreed to modify disclosure requirements "to address the Administration's concerns" regarding constitutional separation of powers issues); *id*. at 28 (stating that the Senate Committee agreed to alter provisions of the Whistleblower Protection Enhancement Act in response to separation of powers concerns raised by the Obama Administration).

475. *See* 5 U.S.C. § 7211 (2006). The definition of "employee" that applies to all of Chapter 5 of the U.S. Code, unless otherwise indicated, does not have an intelligence community exception. *See* 5 U.S.C. § 2105 (2006). The exclusion for intelligence community employees comes from the WPA, which is located in Section 2302 of Title 5 and describes "prohibited personnel practices" for employees of only certain, non-intelligence, agencies. *See* 5 U.S.C. § 2302(a)(2)(C) (2006). Thus, intelligence community employees have a "right" to give information to Congress, but no remedy if the agency retaliates against them for doing so.

476. Kitrosser, *supra* note 170, at 917-18.

477. *Id*. at 918; *see also* Kitrosser, *supra* note 271, at 522-27.

whole of government, domestic and foreign."[478] Moreover, this concept is not new. In 1976, Professors Halperin and Hoffman examined the various constitutional powers assigned to Congress and the President and determined that they "necessarily imply independent but concurrent efforts by the respective branches on behalf of national security interests."[479] Congress provided employees in other areas the ability to give information directly to Congress, and it should expand that right to national security employees as well.[480] The constitutional arguments for presidential secrecy in the national security arena may be persuasive when arrayed against the *public*'s need for transparency.[481] However, when pitted against transparency to *Congress* to assist with its constitutional oversight responsibilities, the President's demands for secrecy should be more circumscribed.

Will Congress do anything with more information? Professor Kitrosser also argued that Congress does not actually want to oversee national security issues because "congresspersons are generally best off appearing tough and resolute, while retaining the ability to plead ignorance should things turn out badly."[482] Similarly, Professor Neal Katyal asserted that Congress has abdicated its responsibility of oversight with regard to foreign affairs.[483] However, as a political matter, more direct, unfiltered infor-

478. *See Protecting the Public from Waste, Fraud and Abuse: Hearing on H.R. 1507, The Whistleblower Protection Enhancement Act of 2009 Before the H. Comm. on Oversight & Gov't Reform*, 111th Cong. 1 (2009) (statement of Louis Fisher, Specialist in Constitutional Law, Law Library of the Library of Congress) [hereinafter Fisher Statement], *available at* <http://democrats.oversight.house.gov/images/stories/documents/20090513183833.pdf>.

479. Halperin & Hoffman, *supra* note 259, at 153.

480. Moreover, part of providing a real outlet to Congress for whistleblowers also would include requirements that national security agencies make clear *how* an employee or contractor should report wrongdoing. *See* GOODMAN ET AL., *supra* note 187, at 20 (recommending that agencies "provide the proper guidance to their employees and contractors so they will know how to report their complaints within the law").

481. *See* U.S. v. Nixon, 418 U.S. 683, 705 (1974).

482. Kitrosser, *supra* note 271, at 484. Kitrosser also has argued that

> The non-public nature of much information funneling means that "Congressional efforts here remain largely hidden" and thus politically unhelpful to its participants. The complexity of much national security information also diminishes its political resonance. Furthermore, the charge that information disclosure will harm national security is easy to make and has substantial popular appeal, making it politically risky to push for disclosures. Indeed, the current [Bush] Administration frequently makes the charge that congressional hearings on national security will provide "the enemy" with valuable information. Fears that the executive branch will intentionally leak national security information and blame Congress for the leak also have been known to exist on Capitol Hill.

Kitrosser, *supra* note 252, at 1084-85 (citations omitted).

483. *See* Neal Kumar Katyal, *Internal Separation of Powers: Checking Today's Most Dangerous Branch from within*, 115 YALE L.J. 2314, 2314 (2005). For Katyal, as a result of this abdication, checks and balances must be accomplished from within the executive branch itself. *See id*. Among other things, he proposes an impartial decision-maker that would resolve inter-agency disputes, *id*. at 2337, an idea seemingly adopted by the government in creating the new IG for the Intelligence Community. This en-

mation from whistleblowers may force Congress to assume its constitutional checking function for fear that not doing so will have greater political ramifications should they ignore the information. As Congress receives better information, it will be harder for it to avoid its oversight role, which can lead to better information for public debate.[484] Moreover, Congress has shown a willingness to undertake official investigations in the past that have pushed for more transparency and served as a countermeasure to the executive branch's tendency for over classification.[485] Further, part of the benefit may be in the deterrent value of whistleblowing.[486] Executive branch actors will know that their decision making may be scrutinized externally, which may lead to better decisions in the first instance.[487]

2. Retaliation Protection

Structural disclosure channels help address information-flow problems because they direct employees to a recipient who might fix the problem identified by the whistleblower.[488] Yet, for employees to report, the law also should address employee fears of retaliation. Although some minimal antiretaliation protection for national security whistleblowers exists now, several flaws should be fixed to truly encourage whistleblowers and remedy any retaliation they experience.[489]

Currently, as set forth in more detail in Part III.B., *supra*, the law contains several prohibitions on retaliation against national security whistleblowers, but little in the way of remedies for any retaliation. For example, the laws creating an IG for the intelligence community and for the CIA bar any reprisals against employees who disclose misconduct to the IG.[490] However, the statutes do not contain any remedy for retaliation, which

hanced internal oversight may prove to be beneficial, for as Stephen Aftergood has argued, "some of the most effective checks and balances on government operations, including new public disclosures of formerly secret information, take place through the process of internal oversight." Aftergood, *supra* note 385, at 848.

484. *See* Aftergood, *supra* note 385, at 847 ("The normal friction that accompanies congressional oversight very often serves as a driver of public disclosure.").

485. *See id*. (giving the Church committee investigations of intelligence activities and the 9/11 Commission as examples).

486. *See* Vandekerckhove, *supra* note 469, at 18 ("The possibility of the second-tier being invoked then serves as a deterrent to the organization.").

487. *Cf*. Christina E Wells, *Questioning Deference*, 69 MO. L. REV. 903, 937-39 (2004) (describing psychological research showing that "accountability can improve judgment and decision making").

488. *See* Moberly, *Structural Model*, *supra* note 440, at 1141-50.

489. *Cf*. Khemani, *supra* note 308, at 4 (concluding that current statutory protections "offer little protection to national security whistleblowers due to narrow judicial interpretations, questionable impartiality of the internal review mechanisms, limited access to external disclosure channels and review bodies, and the lack of effective remedies").

490. *See* 50 U.S.C. § 403-3h(g)(3)(B) (2006) (IC IG); *id*. § 403q(e)(3)(B).

leaves national security whistleblowers without much security. Some whistleblowers may have administrative remedies available to them, such as under the act addressing FBI whistleblowers,[491] or the Military Whistleblowers Act.[492] However, these remedies have not worked well in practice: a recent internal Pentagon investigation determined that the Department of Defense's administrative procedures often failed to adequately protect military whistleblowers.[493] Moreover, these procedures do not provide the due process available to other federal government whistleblowers under the WPA: hearings in front of the Merit Systems Protection Board, with an appeal to the Federal Circuit.[494] If a Whistleblower Protection Enhancement Act passes along the lines of the bills that have been proposed recently, many whistleblowers currently covered by the WPA (but still excluding intelligence community whistleblowers) would be able to bring *de novo* claims in federal district court if the MSPB does not resolve their claim within 270 days.[495]

National security whistleblowers should be treated equivalently to other types of federal whistleblowers regarding the substantive and procedural remedies for retaliation. Originally, the WPA excluded intelligence agencies from its coverage "because the intelligence community handles highly classified programs and information that must be closely guarded from public disclosure."[496] However, the concern that retaliation protection for national security whistleblowers would undermine secrecy confuses two distinct concepts of antiretaliation law: the protected disclosure and the prohibited retaliation. As an initial matter, the law could require national security whistleblowers to maintain the secrecy of their disclosures under the rules set forth by the classification regime. *In addition*, once a whistleblower makes a protected disclosure appropriately, the law could protect the whistleblower from retaliation with a full, or slightly modified, set of remedies.

491. *See* 5 U.S.C. § 2303(b) (2006); 28 C.F.R. pt. 27 (2011).

492. 10 U.S.C. §§ 1034(c)-(g) (2006).

493. *See* Inspector General, U.S. Dep't of Def., Assessment Report: Review of the Office of Deputy Inspector General for Administrative Investigations, Directorate for Military Reprisal Investigations 16 (May 16, 2011), *available at* <https://www.documentcloud.org/documents/351491-dod-ig-internal-review-of-whistleblowing.html> (last visited June 23, 2012); *see also* Tom Vanden Brook, *Report: DoD Delays Endanger Whistle-blowers*, USA Today, Feb. 22, 2012, *at* <http://www.usatoday.com/news/military/story/2012-02-22/pentagon-whistle-blower-delays/53198210/1>.

494. *See* 5 U.S.C. § 1221 (2006) (permitting right of action to MSPB); *id*. § 7703(b)(1) (providing for review of MSPB decisions by the U.S. Court of Appeals for the Federal Circuit).

495. *See, e.g.*, Whistleblower Protection Enhancement Act of 2011, S. 743, 112th Cong., § 117.

496. S. REP. NO. 111-101, at 29 (2009); *see also* Fisher Statement, *supra* note 478, at 18 (describing Justice Department arguments that national security whistleblower legislation would impede upon the President's right to determine who has a need to know classified information).

Therefore, although the disclosure itself could involve classified material, the focus in a retaliation case would be on whether the disclosure caused retaliation – a determination unlikely to involve using details from properly classified materials. The underlying merits of the disclosure (i.e., whether the misconduct reported actually violated the law, which may involve classified information) should not be litigated in a whistleblower case because retaliation law requires only a reasonable good faith belief that the conduct was improper.[497] IGs and internal processes can handle the investigation of the merits of the disclosure separately from the issue of whether the agency retaliated against the whistleblower.[498] Courts and adjudicatory bodies would not be involved in second-guessing executive branch decisions regarding national security – they would only determine whether the agency retaliated against an employee for a protected disclosure.

In some cases, the employee or the agency may need to use classified material as part of the claim or defense. Accordingly, new antiretaliation provisions would have to account for maintaining the secrecy of information throughout the adjudication process. However, such systems could be created. Administrative law judges or hearing officers could be cleared for classified information, and evidence could be presented under seal or redacted. Currently, Title VII claims from intelligence community employees receive this type of treatment to protect sensitive information because the law permits them to file *de novo* claims for discrimination and retaliation in federal court.[499] Importantly, these precautions work for Title VII claims; in 1996 the Government Accounting Office (GAO) studied such claims by intelligence community employees and determined that the claims did not compromise national security.[500] The intelligence agencies successfully removed or redacted classified information from adverse action case files, and the GAO determined that agencies often could litigate the case with unclassified documents.[501]

The version of the WPEA endorsed by *candidate* Obama in 2007, H.R. 985 from the 110th Congress, contained provisions that seemed to

497. *See Protecting the Public from Waste, Fraud and Abuse: Hearing on H.R. 1507, The Whistleblower Protection Enhancement Act of 2009 Before the H. Comm. on Oversight & Gov't Reform*, 111th Cong. 13 (2009) (statement of David K. Colapinto, Nat'l Whistleblowers Ctr.) ("What is at issue in a retaliation case is whether an employee made a protected disclosure . . . and once that is established there is no in-depth examination of the underlying merits of the whistleblower allegations in the retaliation case."), *available at* <http://democrats.oversight.house.gov/images/stories/documents/20090513184228.pdf>.

498. *See id*.

499. *See* 42 U.S.C. § 2000-e (2006); *id*. § 1981a.

500. U.S. GEN. ACCOUNTING OFFICE, GAO/NSIAD-96-6, INTELLIGENCE AGENCIES: PERSONNEL PRACTICES AT THE CIA, NSA, AND DIA COMPARED WITH THOSE OF OTHER AGENCIES 45 (1996).

501. *See id*. at 38-39.

provide the necessary balance between protecting the security of the disclosure and providing a true remedy for retaliation. The law would have protected national security whistleblowers who disclosed wrongdoing to an authorized member of Congress (or a congressional staff member with appropriate security clearance), an authorized executive branch official, or an IG.[502] Whistleblowers who felt retaliated against could submit a complaint to the IG and the agency head, and the IG would investigate and report to the agency head within 120 days.[503] The agency head would have 180 days to make a determination about whether retaliation occurred, and after that the employee could bring a *de novo* claim in federal court.[504] H.R. 985 also would have prohibited the revocation of a security clearance as retaliation, an important additional protection not found in the current laws related to national security whistleblowing.[505] Further, the bill would have limited the ability of the executive branch to claim the "state secrets" privilege in a whistleblower case and required a report to Congress whenever the government asserted the privilege in a case.[506]

The most recent iterations of the WPEA in the 112th Congress, S. 743 and H.R. 3289, fall short of these protections. Although the bills provide more protection from retaliation for national security whistleblowers than currently exists, the protection is more limited than it needs to be. For example, the bills protect national security whistleblowers who disclose misconduct only to the Director of National Intelligence or the head of their agency.[507] This limited disclosure channel does not provide for reporting wrongdoing outside of the intelligence community, thus avoiding any meaningful oversight from Congress. Moreover, the bills do not provide any detail regarding how a whistleblower can enforce the antiretaliation protections. Instead, Congress appears willing to let the executive branch

502. *See* Whistleblower Protection Enhancement Act of 2007, H.R. 985 110th Cong. § 10(a).

503. *See id*. § 10(b).

504. *See id*. § 10(c).

505. The MSPB has determined that it does not have authority to review an agency determination to revoke an employee's security clearance. *See* Hesse v. Dep't of State, 217 F.3d 1372, 1380 (Fed. Cir. 2000). The Obama Administration would have appeals of security clearance revocation go to an extra-agency review process rather than federal court, and if the process recommends reinstated the security clearance, then the law could require notification of Congress if the recommendation is not followed by the agency head. *See* De House Statement, *supra* note 195, at 9-10.

506. H.R. 985 required a court to find in favor of an employee on an element or claim if a "state secrets privilege" claim prevented the employee from proving the element or claim, as long as the IG investigation substantially confirmed the element or elements of the claim. *See* H.R. 985, 110th Cong. § 10(c) (2007).

507. *See, e.g.*, Whistleblower Protection Enhancement Act of 2011, S. 743, 112th Cong. § 201. The House bill, H.R. 3289, presents identical provisions under identical section numbers. *See* Whistleblower Protection Enhancement Act of 2011, H.R. 3289, 112th Cong. Title II.

provide a regulatory scheme "consistent with" the WPA[508] that permits appeals only to a specially appointed board consisting of intelligence community officials.[509] Moreover, the bills subject security clearance revocations to an internal administrative review process involving the same board.[510] Finally, the proposed laws would authorize the Director of National Intelligence to summarily fire employees and to ignore other laws prohibiting the termination of employment when necessary for "national security."[511]

The dearth of retaliation protection currently makes any proposal for added protection sound good. Indeed, given the current limits of statutory protection when national security whistleblowers use official channels, the system ironically encourages employees to disclose wrongdoing to the press or to sources like WikiLeaks in the hope of remaining anonymous. If a new statute protected disclosures deemed appropriate by the classification regime (such as to Congress, the IG, or an agency head), then the system would encourage appropriate secrecy rather than undermine it. However, the system for protecting against retaliation does not need to be as restrictive as proposed by the bills in the 112th Congress. Permitting adjudication and review of retaliation claims outside the intelligence community would provide less conflicted oversight of the antiretaliation system and likely engender more confidence among employees.

3. Whistleblowing as a Duty

Finally, the law often imposes an obligation to report wrongdoing when "the victim of misconduct is particularly vulnerable or the harm will be widespread."[512] A wide variety of employees, from corporate officers and lawyers to supervisors of facilities that handle hazardous materials have an obligation to disclose harmful activity if they witness it.[513] Experimental evidence supports emphasizing the "duty" model to better encourage employees to blow the whistle, particularly when an employee would perceive the illegal conduct to be reported as morally offensive.[514] Moreover, by imposing a duty to report, the law can express to all employees, and the outside world, "an important message of the social desirability of whis-

508. *See, e.g.*, S. 743, 112th Cong. § 201.
509. *See, e.g.*, *id*. § 204.
510. *See, e.g.*, *id*. § 202.
511. *See, e.g.*, *id*. § 204.
512. Feldman & Lobel, *supra* note 440, at 1163.
513. *See id*. at 1163-66 (providing numerous examples).
514. *See id*. at 1155.

tle-blowing."[515]

The current system imposes a duty on intelligence community employees to blow the whistle on illegal conduct. For example, the federal government's Code of Ethics adopted by Congress in 1958 requires all employees to "expose corruption wherever discovered" and to "uphold the Constitution, laws, and legal regulations of the United States."[516] The Standard of Conduct for executive branch employees requires employees to "disclose waste, fraud, abuse, and corruption to appropriate authorities."[517] Federal government employees must take an oath to "support and defend the Constitution of the United States."[518] Anecdotal evidence suggests that these oaths can have some power. For example, Thomas Drake asserts that the oath he took as a federal employee influenced his decision to blow the whistle on mismanagement and waste in the NSA.[519]

Yet, these oaths might conflict with secrecy oaths and written nondisclosure agreements required by intelligence agencies.[520] A national security whistleblower may be confronted with having to decide which oath takes precedence: the oath to expose wrongdoing and uphold the Constitution, or the secrecy promise made when joining the intelligence community.[521] Daniel Ellsberg argued that part of the reason government officials keep

515. *See id*. at 1185.

516. *See* Code of Ethics for U.S. Government Service (1958), *available at* <http://usgovinfo.about.com/blethics.htm>; *see also* Fisher Statement, *supra* note 478, at 2.

517. U.S. Office of Gov't Ethics, Standards of Ethical Conduct for Employees of the Executive Branch 2 (2009), *available at* <http://www.usoge.gov/Laws-and-Regulations/Employee-Standards-of-Conduct/Standards-of-Ethical-Conduct-for-Employees-of-the-Executive-Branch-(June-2009)-(PDF)/>.

518. 5 U.S.C. § 3331 (2006).

519. *See* Thomas Drake, *Why Are We Subverting the Constitution in the Name of Security?*, WASH. POST, Aug. 25, 2011, at A13 ("I followed all the rules for reporting such activity until it conflicted with the primacy of my oath to defend the Constitution."); *see also* Vic Walter & Krista Kjellman, *NSA Whistleblower Now Silent*, ABC NEWS (July 31, 2006, 4:00 PM), <http://abcnews.go.com/blogs/headlines/2006/07/nsa_whistleblow-2/> (reporting that Russell Tice sent a letter to Congress revealing NSA eavesdropping and stating "It was with my oath as a U.S. intelligence officer to protect and preserve the U.S. Constitution weighing heavy on my mind that I reported acts that I know to be unlawful and unconstitutional").

520. *See* FISHER, *supra* note 246, at 24-29 (discussing nondisclosure agreements); Jeff Stein, *CIA Director Panetta Warns Employees on Leaks*, Wash. Post., Nov. 8, 2010, at B3, *available at* <http://voices.washingtonpost.com/spy-talk/2010/11/cia_director_panetta_warns_emp.html> (quoting CIA Director Leon Panetta reminding CIA officers about their "secrecy oath, which obligates us to protect classified information while we serve at the Agency and after we leave").

521. *See* David Canon, *Intelligence and Ethics: CIA's Covert Operations*, 4 J. LIBERTARIAN STUD. 197, 201-02 (1980) (describing conflict some CIA agents felt between CIA's secrecy oath and oath to tell the truth to Congress); Blahblog, *National Security Agency Security Oath*, BLOGMOUTH (July 30, 2008), <http://blogzenze.com/blogmouth/2008/07/30/national-security-agency-security-oath/> ("I solemnly swear that I will not reveal to any person any information pertaining to the classified activities of the National Security Agency, except as necessary toward the proper performance of my duties or as specifically authorized by a duly responsible superior known to me to be authorized to receive this information.").

secrets about misconduct relates to the psychology of keeping promises of confidentiality in return for being permitted to be a part of an elite, secret-keeping group.[522] The secrecy oaths and nondisclosure agreements become part of the enforcement mechanism that, according to Ellsberg, has "the same psychosocial meaning for participants as the Mafia code of *omertà*."[523]

The law should be clear that exposing governmental waste, abuse, and illegality takes precedence over any contractual obligation to keep information secret. The versions of the Whistleblower Protection Enhancement Act in the 112th Congress might help make this unambiguous. The most recent bills contain provisions that require each executive branch nondisclosure agreement to state explicitly that the agreement incorporates and does not undermine the various whistleblower laws and regulations that affect national security whistleblowers.[524] Although these bills have other shortcomings, the provisions related to these nondisclosure agreements should be retained and implemented. Acknowledging the priority of one's duty to report over the duty of secrecy can reduce the conflict between these opposing obligations and make employees more willing to report misconduct.[525]

Importantly, the WPEA bills also contain a requirement that heads of agencies inform employees how they can make lawful disclosures of misconduct when the disclosure includes classified information.[526] Moreover, the bills require each IG to appoint a Whistleblower Protection Ombudsman to educate employees about antiretaliation protections.[527] Oddly, however, the bills exclude the intelligence agencies from this requirement,[528] an exclusion that should be withdrawn in order to give all executive branch employees information about their duty to blow the whistle. Even without this requirement, some agencies have begun to provide clearer direction to their employees regarding how to report misconduct. On October 12, 2011, the Department of Homeland Security issued a proposed rulemaking in which DHS employees would be required to report allegations of waste, fraud, abuse, or corruption to "appropriate authorities within DHS, such as the DHS Office of Inspector General, the appropriate Office of Internal Af-

522. Ellsberg, *supra* note 243, at 777-78.

523. *Id*. at 780.

524. *See, e.g.*, Whistleblower Protection Enhancement Act of 2011, S. 743, 112th Cong. §§ 104, 115.

525. *See* BOK, *supra* note 12, at 228.

526. *See, e.g.*, Whistleblower Protection Enhancement Act of 2011, S. 743, 112th Cong. § 112.

527. *See, e.g.*, *id*. § 120.

528. *See, e.g.*, *id*.

fairs, or Office of Professional Responsibility."[529]

Any duty to blow the whistle should correspond with antiretaliation protection that applies when a whistleblower acts pursuant to this reporting obligation. Courts have held that reporting misconduct as part of one's job duty can eviscerate First Amendment and WPA protection from retaliation.[530] In response to these rulings, the WPEA bills also contain provisions rejecting these courts' "job duty" exception for both WPA whistleblowers and national security whistleblowers.[531] These provisions also should be retained.

Utilizing the "duty model" can be effective, but only if the law makes clear to national security employees that the duty to expose misconduct takes priority over the duty of secrecy. To the extent possible, employees should not receive conflicting messages about these dual obligations. However, the law also can make clear that disclosing classified information as part of a whistleblower report should be accomplished in a way that protects the secrecy of the information. The disclosure channels and antiretaliation protections mentioned above work together with this duty to provide a multi-faceted and consistent approach to supporting whistleblower disclosures, while also respecting the need for secrecy regarding national security matters.

4. Extreme Cases

Reforming the three models currently used to address national security whistleblowers can greatly improve the balance between transparency and secrecy by providing more oversight without significantly threatening important secrecy concerns. The law could funnel disclosures to appropriate legislative and executive branch officials without making classified information public. Moreover, the law could remedy retaliation while still respecting important classification concerns. Various versions of the WPEA introduced in Congress over the last few years would improve the current system tremendously. These improvements would encourage disclosures of low-level, or even agency-wide, abuses because people outside the agency would receive information about the misconduct. These recipients would, presumably, correct the misconduct because of their oversight responsibilities.

529. *See* Supplemental Standards of Ethical Conduct for Employees of the Department of Homeland Security, 76 FED. REG. 63,206, 63,207 (proposed Oct. 12, 2011).

530. *See* Garcetti v. Ceballos, 547 U.S. 410, 421 (2006) (First Amendment); Huffman v. Office of Personnel Mgmt., 263 F.3d 1341, 1352 (Fed. Cir. 2001) (WPA).

531. *See, e.g.*, Whistleblower Protection Enhancement Act of 2011, S. 743, 112th Cong. §§ 101, 202.

However, what about the extreme cases involving more wide-spread extra-agency wrongdoing or misconduct authorized by the President? As Professor Stephen Vladeck noted, internal whistleblowing channels like those provided by the IG Act and the ICWPA "may not be enough when the relevant program has been approved at the highest levels of the Executive Branch, or when there are other reasons to doubt the impartiality of the relevant Inspector General or the Special Counsel."[532] Moreover, disclosure to Congress only matters if Congress can do something about the disclosure publicly, which is not always the case.[533] What if a national security whistleblower discloses classified misconduct to the appropriate congressional recipient, but nothing happens?

Vandekerckhove's three-tier model would suggest that a whistleblower should be permitted to disclose matters of public concern directly to the public if unsuccessful with initial disclosures to the first and second tiers.[534] Otherwise, the executive and legislative branches would not have any accountability "to the wider society" regarding how they address concerns being raised within the branches.[535] In fact, the WPA currently protects disclosures of non-classified information to the media, supporting the three-tier model. However, Vandekerckhove did not address national security issues specifically and, as demonstrated above, such disclosures might require a different balancing than other disclosures.

Despite those secrecy concerns, good reasons exist not to have a wholesale prohibition on national security whistleblowing to the public. An unrestricted ban ignores the public interest side of the transparency-secrecy equation.[536] Moreover, public debate on these issues may be *more* important than on any other, and sometimes leaving oversight to Congress will not be sufficient.[537]

Accordingly, Professor Michael Scharf and Colin McLaughlin suggest that retaliation protection also should be provided to whistleblowers who disclose national security information to the *media* under limited circumstances: if the whistleblower has a "reasonably good faith belief that her allegations are accurate and that the disclosure is necessary to avoid serious

532. Vladeck, *supra* note 296, at 1535.

533. *See id*.

534. *See* Vandekerckhove, *supra* note 469, at 18.

535. *See id*.; Halperin & Hoffman, *supra* note 259, at 141 (arguing that government officials who learn about illegal conduct have an obligation to make that information public).

536. *See* A.J. Brown, *Flying Foxes and Freedom of Speech: Statutory Recognition of Public Whistleblowing in Australia*, *in* WHISTLEBLOWING AND DEMOCRATIC VALUES 86, 94 (David Lewis & Wim Vandekerckhove eds., 2011).

537. *See* BOK, *supra* note 12, at 203 ("Neither committees nor legislative groups meeting in secret to oversee clandestine practices offer sufficient guarantees of accountability.").

harm," the whistleblower has "exhausted internal procedures unless she reasonably believes that disclosure would subject her to retaliation, or that the employer would conceal or destroy the evidence if alerted," and the whistleblower "publicly identifies herself as the source of the information."[538] This suggestion has the benefits of protecting disclosures of only the most serious harms to the public and requiring a whistleblower to utilize the first two tiers of disclosure channels before resorting to the media as a last option.[539] Indeed, permitting extreme cases to be disclosed to the media (acting as a proxy for the public at large) serves as an incentive for the government to take seriously a commitment to receiving whistleblower disclosures and remedying the misconduct whistleblowers identify.[540]

However, the information disclosed should be more strictly defined than Scharf and McLaughlin proposed. They suggested that "the harm in question could be physical (e.g., death, disease, or physical abuse), financial (e.g., loss of or damage to property), or psychological (e.g., invasion of privacy, or inducing terror), but lower level harms (e.g., injustice, deception, and waste) would under most circumstances not be sufficient to meet this standard."[541] Although I agree with the goal of only permitting reports to the media of truly "serious" harms, their standard seems too loosely defined to give much predictive value. Instead, the protections should be limited to disclosures about illegality,[542] where the public interest is the highest[543] and when the information should not have been classified initially. Like other Executive Orders related to classification, President Obama's EO 13,526 makes clear that classification may not be used to conceal viola-

538. Scharf & McLaughlin, *supra* note 239, at 579-80; *see also* Khemani, *supra* note 308, at 27 (asserting that "disclosure to the media should only be protected if it is used as a last resort").

539. Porter Goss has argued that "[t]hose who choose to bypass the law and go straight to the press are not noble, honorable or patriotic. Nor are they whistleblowers. Instead, they are committing a criminal act that potentially places American lives at risk." Goss, *supra* note 408, at A25. However, my suggestion assumes one does not "go straight to the press" but rather has tried to disclose the misconduct to the first two tiers available and has been unsuccessful at having the misconduct addressed.

540. Congress might need to amend the Espionage Act to clarify that it does not prohibit the media from receiving and publishing information appropriately received from whistleblowers under any such provision. *See* Harold Edgar & Benno C. Schmidt, Jr., *The Espionage Statutes and Publication of Defense Information,* 73 COLUM. L. REV. 929, 1000 (1973) (describing arguments that Espionage Act could be interpreted to apply to media disclosures of classified information); Mayer, *supra* note 7, at 57 (noting scholarly arguments that Espionage Act was meant to prevent spying, not mere publication of information).

541. Scharf & McLaughlin, *supra* note 239, at 580.

542. *See* BOK, *supra* note 12, at 130-31 (arguing that professionals with a duty of confidentiality should still breach secrecy obligations "where serious harm is likely to occur"). Similarly, Daniel Ellsberg suggests that whistleblowers who reveal "criminal behavior" to the press should be immune from prosecution. *See* Ellsberg, *supra* note 243, at 799.

543. *See* Richard Moberly, *The Supreme Court's Antiretaliation Principle*, 61 CASE W. RES. L. REV. 375, 382 (2011) (arguing that the Supreme Court broadly interprets retaliation statutes because of society's interest "in having the law enforced").

tions of law, inefficiency, administrative error, or to prevent embarrassment to the government.[544] Limiting the disclosures to information that should not have been classified in the first place because it covered up illegality provides an appropriately high burden for the whistleblower (thus discouraging disclosures without sufficient public value) while also recognizing that the classification system serves as the distinguishing feature between national security whistleblowers and other whistleblowers.[545] If the classification system was inappropriately invoked to hide wrongdoing, then it should not prevent whistleblowers from disclosing the information to the public in order to expose the misconduct.[546] The whistleblower should bear the burden of proving improper classification in order to give appropriate deference to the classification process and to protecting important secrecy concerns.

Unlike the reforms related to improved disclosure channels to Congress, stronger antiretaliation protections, and bolder statements about a government employee's duty to report misconduct, neither Congress nor the President appear interested in making it easier to disclose national security information to the media, even under the limited circumstances suggested above. Notably, President Obama does not stand alone politically in his quest to punish leaks of national security information. Democratic Senator Benjamin Cardin introduced legislation to make prosecuting leakers easier by prohibiting the disclosure of any type of classified document – currently the law only prohibits publishing certain categories of intelligence, such as information related to communications technology or nuclear weapons.[547] The WikiLeaks disclosure of thousands of Afghanistan war documents led to a vitriolic congressional response across the political spectrum: two Democratic Senators scrutinized a bill that would have provided broader protections for reporters who refused to reveal confidential sources in order to ensure that the bill would only apply to "traditional" news sources and not Web sites like WikiLeaks.[548] A Republican Representative asked the State Department to consider WikiLeaks a terrorist group,[549] and a Democratic Senator wanted espionage charges brought

544. *See* Exec. Order No. 13,526, § 1.7, 75 Fed. Reg. 707 (Dec. 29, 2009).

545. *Cf*. Kitrosser, *supra* note 170, at 930 ("[J]udgments as to legal impropriety [of disclosure] should not follow automatically from the facts of classification and disclosure.").

546. *Cf*. BOK, *supra* note 12, at 133 (arguing against confidentiality when used purely as "a means for deflecting legitimate public attention").

547. *See* Espionage Statutes Modernization Act of 2011, S. 355, 112th Cong.; *see also* Benjamin, *supra* note 155.

548. Charlie Savage, *After Afghan War Leaks, Revisions in a Shield Bill*, N.Y. TIMES, Aug. 3, 2010, at A12.

549. *See* Shane, *supra* note 151.

against WikiLeaks' founder Julian Assange.[550]

However, other countries have taken a different view and have provided exemptions to laws prohibiting disclosure of state secrets if the disclosure is in the public interest and it does not damage national security.[551] Some countries, such as Luxembourg, require a showing that the person who disclosed the information intended to damage national security.[552] Moldova and Georgia specifically require a balancing of the public interest against the damage to national security.[553]

Regardless of the approach, the law should account for unusual or extreme circumstances in which both executive branch and congressional actors fail to act appropriately on valid whistleblower disclosures. Ultimately, in those very few circumstances when government actors seem united to hide illegal government conduct, transparency to the public should overcome the natural presumption of secrecy in national security matters.

V. CONCLUSION

Given the competing principles and factual varieties, can we truly balance secrecy and transparency with the law related to national security whistleblowers? These are complex issues, and cases like Thomas Drake should make Congress and President Obama reconsider whether the current balance skews too far toward hiding important information about misconduct from Congress and the public. Statutory whistleblower provisions either exclude national security employees explicitly or only half-heartedly encourage them to blow the whistle on misconduct. By erecting ineffective measures, perhaps we have failed to address either branch's concerns because the law neither fully encourages whistleblowers to go to Congress nor adequately maintains the secrecy that is needed for some state secrets.

Other reforms could increase transparency and address some of the flaws in the secrecy system. With regard to the over classification problem, the law could make it easier for employees to object to information being classified and to protect them from retaliation when they do.[554] The Espionage Act could be amended to make prosecuting whistleblowers more dif-

550. *See id.*

551. *See* DAVID BANISAR, LEGAL PROTECTIONS AND BARRIERS ON THE RIGHT TO INFORMATION, STATE SECRETS AND PROTECTION OF SOURCES IN OSCE PARTICIPATING STATES 22 (2007) (providing examples such as Denmark and Austria).

552. *See id.*

553. *See id.*

554. Obama has taken steps to reduce the chronic overclassification problem. For example, he established the National Declassification Center to expedite declassification decisions. *See* Exec. Order No. 13,526, § 3.7, 75 Fed. Reg. 707 (Dec. 29, 2009).

ficult by requiring the prosecution to prove the whistleblower meant to harm national interests and by permitting a defense that the information released was improperly classified because, for example, it was classified in order to conceal illegality or embarrassing information.[555] Congress could provide reporters a statutory privilege not to reveal sources.[556] Legislation could limit the use of the state secrets doctrine to avoid civil lawsuits by whistleblowers.[557] Entire articles can be, and have been, written on these topics. For now, I just note that there are many moving parts to the issue of how best to encourage transparency and to protect needed secrecy. A comprehensive approach does not appear forthcoming, but perhaps if Congress and the President address the needs of national security whistleblowers by strengthening the models described above, then other reforms may follow.

555. Stephen Vladeck and others have suggested a statute specifically designed to address leaks to the media, including a provision permitting a defendant to argue that the information leaked should not have been classified as secret. *See* Halperin & Hoffman, *supra* note 259, at 145 (arguing, in 1976, that the law should prohibit any criminal sanction or administrative penalty for someone who releases improperly classified information); Shane, *supra* note 9 (quoting Vladeck). Currently, classification may not be used to conceal violations of law, inefficiency, administrative error, or to prevent embarrassment to the government. *See* Exec. Order No. 13,526, § 1.7, 75 Fed. Reg. 707 (Dec. 29, 2009).

556. *See, e.g.*, Jonathan Peters, *WikiLeaks Would Not Qualify to Claim Federal Reporter's Privilege in Any Form*, 63 FED. COMM. L.J. 667, 688-94 (2011) (describing congressional legislation related to a proposed reporter's privilege).

557. *See* GOODMAN ET AL., *supra* note 187, at 20.

8 J.L. Econ. & Pol'y 83

Journal of Law, Economics & Policy
Fall, 2011

Comment

WHISTLE-BLOWING IN THE INTELLIGENCE COMMUNITY: WHY A NEW BOARD WILL BE A STEP IN THE RIGHT DIRECTION

Andrew Galle[a1]

Introduction

On February 14, 2006, Lt. Col. Anthony Shaffer made a statement to the House of Representatives that encapsulates the current problem that whistle-blowers in the Intelligence Community (IC) face.[1] Shaffer explained that part of his duties as an intelligence operative with the Defense Intelligence Agency (DIA) required him to work on a project named "Able Danger," which was designed to disrupt Al Qaeda operations shortly before the 9/11 terrorist attacks.[2] From his unique position inside the operation, Shaffer observed mismanagement of intelligence resources so severe that he believed it allowed the 9/11 tragedy to occur.[3] In 2003, he disclosed these allegations to Congress in an effort to prevent mismanagement by the DIA from leading to similar attacks in the future.[4] Even though then-current law protected his ability to make such disclosures,[5] the DIA revoked Shaffer's security clearance within forty-eight hours of his disclosure, effectively ending his career.[6] The DIA told Shaffer that his security clearance was revoked because of several administrative irregularities, such as the occasional work-related twenty-five cent charge on his government phone and his high school marijuana use, which curiously became a career-ending issue even though it had not been in the fifteen-plus years since he admitted to the behavior.[7] Shaffer had nowhere to turn to seek meaningful review of the retaliatory revocation of his security clearance, which was ***84** obviously based on pretextual justifications and intended to silence him.[8] The result of incontestable terminations such as this was to generate an atmosphere of "abhorrent . . . values" within the DIA, where employees focused on "self preservation and obfuscation of responsibility," rather than their mission of safeguarding the nation.[9]

Shaffer faced two main problems that continue to plague the IC. First, intelligence workers have no meaningful forum for review of potentially retaliatory revocations of their security clearances. Second, intelligence workers having knowledge of mismanagement have no incentive to come

forward, do the right thing, and make disclosures that could save lives. These employees may even take matters into their own hands and leak the information to anyone who will listen.[10] Without eliminating these problems, people like Lt. Col. Anthony Shaffer will remain victims of retaliation, those who fear for their job security will not make critical disclosures, and national defense will ultimately suffer as mismanagement will continue to place the nation at risk for tragedies like 9/11.

However, a proposed piece of legislation may provide the solution to these problems. In 2009, Senate bill S. 372, also known as the Whistleblower Protection Enhancement Act of 2009 (WPEA), was released from committee and scheduled for consideration.[11] An ambitious piece of legislation, S. 372[12] proposes the creation of the Intelligence Community Whistleblower Protection Board (ICWPB), a forum that would extend traditional whistle-blower protections to IC whistle-blowers and finally provide a meaningful place for security clearance retaliation complaints to be heard.[13] While S. 372 does not currently provide significant incentives for IC whistle-blowers to come forward with critical disclosures, it does create a useful framework for such a scheme in the future.[14]

This Comment has two purposes: (1) to survey the current state of whistle-blower protections in the IC; and (2) to analyze if the creation of ***85** the ICWPB can achieve the socially optimum level of whistle blowing. It will first describe the historical tug-of-war among the branches of government over the authority to make reforms in this field, the current pathways available to IC whistle-blowers, and the enhancements proposed by S. 372. Next, it will assess the effectiveness of the current system and the legal challenges that face any proposals to improve the system. It will then explore efficiency concerns and argue that the benefits of increasing whistleblower protections to intelligence workers outweigh the costs of not doing so. It will also recommend the creation of the ICWPB and include suggestions on how the proposal can be improved. Finally, this Comment will conclude that although the ICWPB, as currently planned, is insufficient to encourage IC whistle-blowers to come forward, it should be created because it provides an ideal framework to which essential upgrades can be added later.

I. Background

A. The Competition Over Information Related to National Security and Why it Frustrates Meaningful Reform

Workers in the IC agencies[15] are fundamentally different from other federal employees primarily because of the nature of their work. Their business requires them to collect, analyze, and disseminate information related to national security.[16] As the handling of information related to national security is inherently dangerous, disclosure of such sensitive information must be properly restricted.[17] However, the workers who deal in this information may discover evidence of theft, waste, and abuse[18] intertwined ***86** with restricted information.[19] Even if an intelligence

worker wanted to blow the whistle after discovering theft, waste, or abuse, the restrictions on the disclosure of such sensitive information may prevent him from doing so.[20] Therefore, to discuss whistle-blower reform in the IC, it must first be determined who is entrusted with placing restrictions on information related to national security.

1. The Executive Interpretation

Article II, Section 1 of the United States Constitution vests the President with the executive power of the nation and compels him to execute his office faithfully.[21] Further, Article II, Section 2 makes the President Commander-in-Chief of the nation's military forces.[22] Taken together, these two provisions show that the Executive Branch has a constitutionally vested interest in providing for the nation's security and enforcing related laws. For the President to be successful in meeting his constitutional mandate, he requires the ability to keep information related to national security secret.[23] For example, a covert operation will yield little information if the enemy it is directed against knows who is involved and what methods are used to gather information.[24] Worse yet, an IC operative whose identity is improperly disclosed may lead to his "incarceration, interrogation, torture and death."[25] Finally, exposed operations within a foreign nation could frustrate diplomatic relations with that nation, especially if American citizens are expelled, peace talks break down, or trade embargos are imposed.[26] In short, without secrecy, the Executive's intelligence operations would be ***87** ineffective, much more dangerous to conduct, and may sour relations with other countries.

The Executive Branch has long argued that because these intelligence operations are so vital to national security, it alone must be the exclusive authority over how information related to national security is classified, restricted, and disclosed. For example, in signing the Intelligence Community Whistleblower Protection Act of 1998 (ICWPA) into law,[27] President Clinton made clear that he was doing so because he did not think that it conflicted with the President's exclusive power to control the disclosure of information related to national security.[28] He explained that the Constitution is the source of this executive power and that Congress cannot interfere with or constrain his ability to exercise this authority through legislation.[29] In a recent statement by Deputy Assistant Attorney General Rajesh De, the Department of Justice made clear that the Obama Administration continues to endorse the idea that Congress cannot interfere with the Executive's exclusive control of national security information.[30] Furthermore, he cautioned Congress that any legislation that would allow it to evaluate determinations on the matter will be viewed as unconstitutional and will not be endorsed by the President.[31] This means that when an executive agency (as an extension of the President) determines that information may only be disclosed to those with a certain security clearance level, no other branch can evaluate the reasonableness of the restriction.[32] Similarly, if an executive agency determines that a person is unfit to receive or maintain his security clearance, then the decision on the matter is incontestable outside of the Executive Branch.

2. The Judicial Interpretation

The Supreme Court of the United States has long recognized that the Executive Branch requires secrecy to accomplish its constitutional mandate to provide national security and enforce related laws. For example, the Court in CIA v. Sims[33] recognized that intelligence operations require secrecy ***88** to be effective, and the failure to maintain secrecy in one instance would reduce effectiveness in the future, as potential sources would "close up like a clam."[34] Commentators have observed that the courts have consistently and pervasively recognized the Executive's need for secrecy when carrying out national security operations.[35]

Courts recognize that secrecy is important to the Executive Branch and acknowledge that control over the disclosure of national security information exclusively resides with the Executive Branch. The Supreme Court made this "exclusive control" doctrine clear in its decision Department of the Navy v. Egan.[36] In Egan, the Navy employed a laborer to perform work on a nuclear submarine.[37] The work he was hired to perform required a security clearance, which he was unable to obtain due to his criminal history.[38] The Navy terminated his employment because his inability to obtain a clearance prevented him from performing the work he was hired to do.[39] The Court found that the Navy could terminate employees for failure to obtain a security clearance when that failure precluded them from performing the work for which they were hired.[40] The Court also found that the Judicial Branch could not review the reasonableness of an adverse security clearance determination that led to the termination.[41] In justifying this holding, the Court observed that executive authority over security clearance determinations "flows primarily from this constitutional investment of power in the President and exists quite apart from any explicit congressional grant."[42] Therefore, because the grant is constitutionally reserved to the Executive Branch, the Legislative Branch cannot pass laws providing for a review of such determinations, and the Judicial Branch cannot perform one. In this way, the Judicial Branch's interpretation of where the Constitution places authority over national security information complements the Executive Branch's interpretation, especially as it relates to the Executive's exclusive authority to issue security clearances.

*89 3. The Legislative Interpretation

Congress, however, rejects the idea that the President has exclusive authority over information related to national security.[43] Even outside the realm of national security, Congress has long insisted that to preserve its constitutionally-created role as a separate and coequal branch of government, a federal worker's ability to bring disclosures of theft, waste, and abuse before Congress must be preserved.[44] One of the earliest examples of this stance can be found in the 1902 debates leading up to the passage of the Lloyd-LaFollette Act of 1912.[45] In 1902, President Roosevelt issued an executive order prohibiting any federal employee from communicating directly with members of Congress.[46] Instead, federal employees with a concern that would require congressional oversight would need to bring the matter to their agency head; if the matter

was worth looking into, the agency head would have access to channels that would lead to Congress.[47] Congress was outraged by this arrangement, feeling that congressional oversight was impossible if the rank-and-file worker was unable to come to Congress with whistle-blowing information.[48] In one congressman's words, the end result would be to reduce the federal government to one "aristocratic Government, dominated completely by the official family of the President."[49] Congress temporarily remedied this problem with the passage of the Lloyd-LaFollette Act of 1912, which prohibited the President from issuing such "gag orders" that would prevent a federal employee from speaking with Congress directly.[50]

As discussed earlier, however, information related to national security is inherently dangerous and treated differently from regular disclosures made by employees. For a federal employee to disclose any classified information to another, a determination must first be made that the recipient, even a senator or representative, "need[s]-to-know" of the information.[51] While it may be the case that Congress has a need to know of information that lies intertwined with national security information, that determination must be made by the agency head, not a rank-and-file intelligence employee. ***90** [52] Thus, even after the Lloyd-LaFollette Act, IC employees effectively remained barred from bringing whistle-blower disclosures before Congress, as any information they came across would likely be intertwined with classified information.

Despite the unique qualities of information related to national security, Congress has firmly maintained that rank-and-file federal workers must be empowered to directly disclose whistle-blowing allegations to Congress so that it may act as an effective check on executive agency wrongdoing.[53] In the ICWPA, discussed in-depth in the next section, Congress made its position clear by enumerating six key points:

(1) national security is a shared responsibility, requiring joint efforts and mutual respect by Congress and the President;

(2) the principles of comity between the branches of Government apply to the handling of national security information;

(3) Congress, as a coequal branch of Government, is empowered by the Constitution to serve as a check on the Executive Branch; in that capacity, it has a "need to know" of allegations of wrongdoing within the Executive Branch, including allegations of wrongdoing in the Intelligence Community;

(4) no basis in law exists for requiring prior authorization of disclosures to the intelligence committees of Congress by employees of the Executive Branch of classified information about wrongdoing within the Intelligence Community;

(5) the risk of reprisal perceived by employees and contractors of the Intelligence Community for reporting serious or flagrant problems to Congress may have impaired the flow of information needed by the intelligence committees to carry out oversight responsibilities; and

(6) to encourage such reporting, an additional procedure should be established that provides a means for such employees and contractors to report to Congress while safeguarding the classified information involved in such reporting.[54]

Interestingly, at the time of the ICWPA's passage, President Clinton found that the legislation did not conflict with the Executive's interpretation of where the Constitution assigns responsibility for controlling information related to national security.[55] However, because the ICWPA allows an IC employee to disclose classified information to Congress, even against the ***91** wishes of his agency head or the President, the legislation erodes the Executive's ability to prevent such disclosures from being made.[56]

B. Pathways to Whistle-blowing

As information related to national security is dangerous, its disclosure must be sufficiently restricted to preserve national security. At the same time, such information must not be so restricted that IC agencies will go without oversight, which could result in agency excesses. Therefore, it is reasonable to treat IC whistle-blowers differently than other federal whistleblowers due to the special restrictions on information related to national security. This explains, in part, why the Whistleblower Protection Act (WPA), the legislation that provides protection for most federal workers, specifically excludes IC workers.[57] Similarly, an IC whistle-blower is generally not permitted to pursue an action under the False Claims Act (FCA), which incentivizes whistle-blowing by awarding him 15%-30% of the waste he prevents or uncovers, because the FCA does not authorize the disclosure of information related to national security.[58]

However, even though the most common and most lucrative pathways to whistle-blowing are closed to intelligence workers, Congress did not intend for these employees to be entirely foreclosed from whistle-blowing. It instituted two main routes to enable whistle-blowing by such workers-the Inspector General system and the ICWPA.[59]

1. The "Ask the Boss" Method: Inspectors General

The Inspector General Act of 1978 (IGA)[60] was one of the first attempts to give whistle-blowers an opportunity to come forward without fear of losing their jobs. An Inspector General (IG) is a presidential appointee, confirmed with the advice and consent of the Senate,[61] whose purpose is to prevent, detect, and report to Congress and agency heads incidents of fraud and abuse within their assigned executive agencies.[62] One way IGs accomplish this charge is by guaranteeing that employees, who come to them ***92** seeking to disclose an incident of theft, waste, or abuse[63] will

not be subject to reprisal unless the disclosure was made "with the knowledge that it was false or with willful disregard for its truth or falsity."[64] It is interesting to note that the President may remove an IG at any time; although Congress must be informed before the dismissal, the IGA does not provide a mechanism for Congress to prevent the removal.[65] Even though Congress could take other actions, such as exercising its spending power or exerting political pressure, they are less convenient to use than a built-in mechanism would be. Currently, each IC agency, like all other federal agencies, has access to an IG.[66]

It is important for the IC whistle-blower to understand that when he chooses this path, it goes no further for him than the IG's door.[67] The whistle-blower is not asking permission to contact Congress with his urgent concerns (doing so is forbidden if the information is classified),[68] but rather he is asking the IG to do so for him while informing the agency head.[69] Should the IG decide the complaint is not credible and not worth mentioning in any of his reports, the whistle-blower's allegations end there and no appeal of the decision is possible.[70] While in those instances the IG must inform Congress and the agency head that he has conducted an investigation, the report need not amount to little more than statistical data.[71]

2. The Direct Approach: The Intelligence Community Whistleblower Protection Act

Congress passed the ICWPA[72] in 1998 to prevent IGs and agency heads from escaping congressional oversight by downplaying the merit of ***93** credible IC whistle-blower reports. The ICWPA provides an IC whistleblower with an alternative path to reach Congress when his agency head or IG did not believe the information to be credible.[73] The employee must still first make a report to his agency's IG, who has fourteen days to determine if the complaint is credible.[74] If the IG finds the report to be credible, the report must be forwarded to the agency head, who has seven more days to provide comments before the report then heads to Congress's intelligence committees.[75] However, if the IG finds that the information is not credible, the whistle-blower may still contact the intelligence committees as long as he informs the IG and the agency head of his intention to do so and complies with all security precautions and instructions in contacting the committees.[76]

The net effect of the ICWPA is to create a path to Congress for the IC whistle-blower who remains concerned about improper agency behavior even after his agency head and IG insist that the information should not reach Congress. In theory, this legislation should have ended the Executive's hegemony over the IC and restored legislative oversight.

3. The WPEA Proposals

In February 2006, the House Committee on Government Reform held hearings entitled "National Security Whistleblowers in the Post-September 11th Era: Lost in a Labyrinth and Facing Subtle

Retaliation,"[77] to determine whether existing whistle-blower protections were adequate for intelligence workers.[78] In these hearings, Lt. Col. Shaffer, whose unfortunate story is recounted in this Comment's introduction, finally had his opportunity to address Congress about the unjust and retaliatory revocation of his security clearance.[79] Other victims of agency retaliation, including Former FBI Special Agent Michael German, joined Shaffer in the hearings.[80] German was an FBI whistle-blower who made allegations against his agency to the Department of Justice's IG, accusing the Bureau of conducting illegal wiretaps and falsifying official documents.[81] His reward for blowing the whistle on his agency was an investigation into his own expense accounts, with an eye ***94** toward revoking his security clearance.[82] After struggling for years with the IG to properly investigate his complaints, German quit the Bureau, disgusted over the IG's disinterest in the FBI's integrity.[83]

The allegations of retaliation reported by German, Shaffer, and others convinced Congress to reform whistle-blower protections for IC workers. Each chamber came up with its own proposal, entitled the Whistleblower Protection Enhancement Act of 2009 (WPEA).[84]

The House version, H.R. 1507, would provide that IC employees "may not be discharged, demoted, or otherwise discriminated against (including by denying, suspending, or revoking a security clearance)" as a reprisal for making protected disclosures of theft, waste, or abuse.[85] Furthermore, should such a reprisal occur, the United States Court of Appeals for the Federal Circuit, or another appropriate federal appellate court, would have jurisdiction to review the alleged prohibited activity.[86] If the reprisal involved a security clearance determination, judicial review would also be available before the Merit Systems Protection Board (MSPB)[87] following an appeal within the whistle-blower's agency. If the MSPB (or the reviewing appellate court) finds that the security clearance determination was made in retaliation of a protected disclosure, the agency would be required to rereview the determination, "giving great weight to the Board or court judgment."[88]

The Senate's version, S. 372, offers similar protections to its House counterpart, but includes different protections against improper review board decisions. Where H.R. 1507 relies on the existing federal appellate courts to hear complaints, S. 372 proposes the creation of a new forum, the ICWPB.[89] As part of the Office of the Director of National Intelligence (ODNI), the ICWPB would be entirely within the Executive Branch.[90] The ICWPB would be composed of one chairperson and four members, two of whom must be IGs.[91] Two alternate IGs would be available in case the issue before the ICWPB affects any of the member IGs' agencies.[92] The ***95** President would appoint each ICWPB member with the advice and consent of the Senate.[93]

An IC employee would be authorized to appeal an adverse personnel action (except a security clearance determination) when he believes he is being retaliated against for making a protected disclosure of theft, waste, or abuse.[94] He would first appeal within his agency according to ICWPB-established procedures, which closely resemble procedures under the WPA.[95] Should the intra-agency appeal result in a finding against the employee, the employee may then appeal to the

ICWPB.[96] If the ICWPB finds against the employee, review is then available in the United States Court of Appeals for the Federal Circuit.[97] In any event, if the reviewer finds against the agency at any level, the employee is to be returned to the position he would have occupied had the prohibited personnel action not injured him.[98] This may be accomplished by ordering the agency to pay reasonable attorney fees, back pay, benefits and compensatory damages not to exceed $300,000,[99] but neither the ICWPB nor the court is authorized to order the agency to reinstate the employee.[100]

If the retaliation is alleged to have involved an adverse security clearance determination, the process is slightly different. The first step is to appeal within the agency and then before the ICWPB, as with other types of prohibited personnel actions.[101] If the ICWPB finds against the whistleblower, then no further appeals are possible.[102] However, should the Board find that the security clearance action was retaliatory, then it shall reinstate the clearance as long as doing so is "clearly consistent" with the interests of national security.[103] Furthermore, though the ICWPB can provide the same remedies to a victim of security clearance retaliation as it could for other offenses, the President can void the ICWPB's remedy if it "would endanger national security."[104]

*96 II. Legal Analysis

The trail of legislation leading up to the WPEA tracks decades of attempts by Congress to convince IC whistle-blowers that it is safe for them to speak out. The Executive Branch similarly claims that whistle-blowers are a vital part of effective government, even if they are blowing the whistle on executive agency abuses.[105] Executive Order 12674 commands all federal employees to report all occurrences of "waste, fraud, abuse and corruption" that they encounter "to appropriate authorities."[106] Despite legislative protections and presidential encouragement, few intelligence workers will raise allegations of theft, waste, or abuse if they are not confident that their careers will be safe.

A. Problems with the Inspector General System

The IG is not always perceived as a safe route to disclosing information.[107] One explanation for this perception can be found in the legislation that created the office. In the IGA, the position of Inspector General is subservient to, not independent of, executive authority.[108] The IG is appointed by the President with the advice and consent of the Senate, but is only removable by the President.[109] Although the President must submit his reasoning for the removal to Congress, the IGA provides Congress with no mechanism to modify his decision.[110] This means that by design, the IG is more dependent on the Executive than Congress for his continued employment, and therefore is more susceptible to the Executive's influence.

Admittedly, some examples tend to show that in practice, IGs behave more independently than the

IGA seems to envision.[111] For example, Inspector General Glenn Fine of the Justice Department produced reports damning the Bush Administration's conduct.[112] One commentator described ***97** Fine's reports as "gripping, if sickening, reading," which "show[ed] a Department . . . that squandered literally hundreds of years of experience and expertise that were acquired and deployed during previous Administrations."[113] If the President truly had absolute control over IGs and Congress was powerless to stop their removal, then the President would presumably fire IGs like Fine. The continued employment of such IGs, even after severely criticizing the Administration, suggests a "soft power" check on the President's removal power. Perhaps presidents fear that adopting draconian personnel policies would sour public opinion. Alternatively, they may be aware that Congress will not cooperate with such an Administration and will pass legislation to change the system if it is abused. Whatever the reason, past practice cannot guarantee future performance. Soft power checks can never be as reliable as actual legislative barriers to executive excesses, and the fact remains that IGs are ultimately accountable to the President.

In fact, there is reason to believe that the Executive's domination of the IG system has caused IGs to resist conducting proper investigations against the Administrations they work under. Recall Former FBI Special Agent Michael German's testimony about the difficulty of convincing the Department of Justice's IG to look into serious and flagrant crimes in the FBI.[114] He complained that it took years of struggling to convince the IG to even start an investigation that later substantiated his claims. Despite his ultimate vindication, German left the Bureau in disgust.[115] Does this IG sound like an individual that is zealously seeking to ferret out corruption, theft, waste, or abuse wherever it can be found? Or does he sound more like an agent of the Executive who is reluctant to reveal his employer's corruption, dragging his feet until the problem employee goes away?

Even some of the IGs' own statements at the 2006 "Lost in a Labyrinth" hearings smack strongly of a disinterested and ineffective office.[116] The primary purpose of the hearings was to investigate the alarming rise in security clearance revocations made in retaliation against whistle-blowers after they made protected disclosures.[117] Yet the IGs who could be reached for comment had never heard that such a problem existed.[118] The CIA's IG, for example, did not even attend the hearings, and declined his invitation ***98** with a letter indicating that he had nothing to add because his office had never heard such a complaint.[119]

Similarly, the Department of Energy's IG reported no substantiated allegations of whistle-blowers being retaliated against by having their security clearances removed.[120] Inspector General Gregory Friedman reported that his office had received three complaints alleging security clearance retaliation in the past ten years, every one of which was resolved in favor of the Department.[121] Furthermore, Mr. Friedman said his office received approximately 10,000 whistle-blower complaints unrelated to security clearance retaliation during the same period, many of which were sustained.[122] How is it that the same agency can be so likely to commit so many abuses, yet never commit security clearance retaliation? One answer may be that security clearance retaliation

actually does occur, but goes largely unreported because it is not subject to meaningful review. This would explain both the incredibly low frequency of complaints alleging security clearance retaliation as well as the unlikely result that the IG will hold the agency responsible. A whistle-blower has little reason to bring a complaint when he has no chance of success.

Most shockingly, Inspector General Glenn Fine reported that the Department of Justice has never received a security clearance retaliation complaint.[123] Mr. Fine's statement was particularly surprising because earlier in the same hearing, Former FBI Special Agent Michael German stated that he had made precisely those allegations. German stated that not only was he the target of a malicious investigation to find a pretext to revoke his security clearance, but he had been struggling with the IG to do something about it for years.[124] Not surprisingly, Mr. Fine's office also did not receive any requests to contact Congress under the ICWPA.[125]

This is not to suggest that the IGs are colluding to ignore whistleblower complaints and protect their executive agency masters in an effort to silence opposition. Neither does it suggest that the IGs conduct poor investigations. Instead, the point is simply that significant evidence exists that would support a perception in the IC community that the IG system is not a safe or effective vehicle for protecting IC whistle-blowers who depend on their security clearances.

*99 B. Problems with the Intelligence Community Whistleblower Protection Act

Because the ICWPA allows IC whistle-blowers to sidestep the IGs and go directly to Congress with their allegations of theft, waste, and abuse, the ICWPA is an important step toward securing congressional oversight of intelligence agency conduct. However, whistle-blowers will only use the provisions if they can be assured that a safe and effective system will protect their post-disclosure careers. As the 2006 "Lost in a Labyrinth" hearings dramatically illustrated, whistle-blowers have ample reason to fear that blowing the whistle under the ICWPA will be the last career move they make.

Lt. Col. Anthony Shaffer testified in those 2006 hearings that he made a disclosure to the 9/11 Commission, alleging that the DIA's mismanagement had allowed the 9/11 tragedy to occur.[126] Because the DIA knew that Egan made security clearances unreviewable outside of the Executive Branch, it was confident that it could pick any pretext it wanted to revoke Shaffer's security clearance.[127] In his case, it was Shaffer's improper call-forwarding, which periodically cost the DIA twenty-five cents, that led the Agency to determine that he was unfit to handle information related to national security--a preposterous conclusion belying the DIA's true motive.[128] However, without meaningful review to shed light on pretextual determinations, the Agency could have chosen virtually any reason at all, no matter how ludicrous.

The Executive Branch rejects such analysis, arguing that meaningful review that prevents retaliatory security clearance revocations is already available.[129] Deputy Assistant Attorney

General Rajesh De explained, in a statement regarding S. 372, that under Executive Order 12968 IC whistleblowers are already guaranteed a "panoply of due process protections."[130] Executive Order 12968 provides that an employee is entitled to an appeal of a security clearance revocation in front of a panel chosen by the agency head.[131] The employee is allowed: (1) to access any documents that led to the revocation to aid in the preparation of the appeal; (2) to be aided by an attorney; and (3) to have any rulings made in writing.[132] However, the protections offered in Executive Order 12968 are unreliable. Any due process protection, or even the right to the appeal itself, is subject to the discretion ***100** of the agency head, whose decisions are final.[133] Even Mr. De conceded that such protections were inadequate and that the President supports a system where review would be conducted outside of the agency that initially denied the security clearance.[134]

The protections currently in place within agencies are admittedly insufficient; even the Executive Branch is concerned about the impartiality of an agency head. Put simply, an IC whistle-blower is ill-advised to make disclosures, as his agency is likely to respond with career-ending retaliation.

C. The Intelligence Community Whistle-blower Enhancement Act (WEA) Proposals

H.R. 1507 is perhaps one of the best ways to guarantee IC whistleblowers access to meaningful review, as it would enable them to appeal to federal courts.[135] The availability of such appeals would mean that personnel decisions, including security clearance revocations, could not be done in clear and obvious retaliation against intelligence employees for making disclosures against their employers. This is because the agency would have to answer to an independent fact finder outside of the Executive Branch, with eventual recourse to life-tenured Article III judges and possibly even the Supreme Court.[136] However, the H.R. 1507 scheme is likely to fail because allowing federal courts to hear appeals of adverse security clearance determinations ignores the Executive Branch's exclusive domain over such decisions.[137] Even though the intelligence agency is not obliged to accept the court's determination and restore a security clearance, it still must "give great weight" to the court's opinion, which improperly invites judicial influence to an area that Egan has made off-limits to the courts.[138] Although Mr. De may have indicated that the Obama Administration was not averse to review outside of the agency making a security clearance revocation, he was adamant that the Constitution mandates that such review must be entirely within the Executive Branch.[139]

S. 372, on the other hand, does not extend itself beyond the Executive Branch.[140] It organizes the ICWPB under ODNI and the President appoints ***101** the Board's membership.[141] Furthermore, when approximately half of the ICWPB's members must be IGs, who the President can remove without congressional approval, there can be no question that the Board is primarily a creature of the Executive.[142] Therefore, Egan would not preclude the Board's existence. Moreover, because the IGs cannot be from the same agency that is the subject of the IC whistle-blower's complaint, the ICWPB appears to be more impartial than the internal agency review provided under Executive Order 12,968.[143] With a greater perception of impartiality, it would follow that

whistle-blowing would be more likely to occur because an IC employee would feel that his agency would have less of an opportunity to retaliate against him.

However, it is important to note that the stigma of agency bias would not completely disappear under S. 372. As long as the entire review process is contained within one branch of government, no check is placed upon executive power, and thus agencies' wrongdoing is not truly curbed under this new scheme. Therefore, while the ICWPB is a step in the right direction, it does not go far enough.

D. The Missing Piece: Incentives

The IGA, ICWPA, and WEA are all styled to provide protections from retaliation for making disclosures, but do nothing to encourage a whistleblower to come forward in the first place. Put another way, aside from keeping his job, the IC whistle-blower does not benefit from whistleblowing, even though such behavior is socially valuable. As commentators have pointed out, enabling an individual to profit from exposing theft, waste, and abuse is the single most effective tool in ending that wrongdoing.[144] The optimum level of incentives is an economic question, to which we turn to next.

*102 III. Economic Analysis

Whistle-blowers provide a socially valuable function but also impose costs on society. First, the complaints whistle-blowers generate must be litigated and resolved by an appropriate authority, which requires funding. Second, especially in the IC, an increase in the level of whistle-blowing activity also increases the risk of exposing information related to national security. Therefore, to determine if the ICWPB can achieve the socially optimum level of whistle-blowing (where the benefits derived from the activity at least equal the costs), we must first identify the costs and benefits.

A. Benefits of Whistle-blowing

1. The IC Can No Longer Control Itself, and IC Whistle-Blowers Provide Self-Policing

The post-9/11 IC is fast becoming synonymous with wastefulness. In the July 2010 "Top Secret America" series of articles in the Washington Post, authors Dana Priest and William M. Arkin revealed the results of their two-year investigation into the shocking expansion of the IC and its troubling lack of transparency.[145] Their findings show that spending in the IC has reached astronomical proportions, reaching its height in 2009 at $75 billion annually.[146] In the past nine years, for example, the equivalent footprint of three Pentagons has been erected in the Washington, D.C. area.[147] Additionally, during that span, at least 263 new organizations were

created to support the IC, bringing the community to an estimated 853,000 workers.[148] The Department of Homeland Security alone commands a workforce of 230,000.[149]

From this mushrooming community comes a work product that is so vast that it is unmanageable to the few individuals in a position to review and absorb it. As one high-level interviewee put it, "I'm not going to live long enough to be briefed on everything."[150] Another official assigned to review and audit portions of the IC concluded that "it inevitably results in ***103** message dissonance, reduced effectiveness and waste, and [I] consequently can't effectively assess whether it is making us [safer]."[151]

Much of the excess volume of information is the result of redundancy within the IC. For example, fifty-one federal organizations all track the monetary transactions between terrorist networks, often duplicating the same work.[152] The reports of one organization are generally ignored by other organizations even if they are shared because agencies prefer to rely on their own in-house information.[153]

Combining unbridled spending with the inability of management to control expenditures results in an opportunity for the unscrupulous to fleece the government. The chances of being noticed, let alone caught, appear to be well in the favor of the defrauder.[154] Further, a thief's odds of succeeding are increased in the IC, as intelligence workers are unwilling to risk their careers by raising allegations in a culture that has been described as unfriendly toward whistle-blowers.[155]

Increasing whistle-blower protections therefore increases the ability of agency management to combat theft, waste, and abuse. Management will no longer need to be as vigilant and proactive in rooting out such wrongdoing if each employee has an incentive to bring wrongdoing to light. Thus, self-policing becomes a very real benefit of allowing whistle-blowing.

2. Discouraging Dangerous Vigilante Whistle-Blowing

Another benefit from providing effective, strong, and reliable whistleblower protections is that such protections discourage well-meaning employees from taking matters into their own hands to expose instances of theft, waste, and abuse. This is because an employee who feels safe blowing the whistle through proper channels (let alone meriting a reward for his good deed)[156] will be less likely to attempt to hide his identity and disclose information related to national security directly to the public, as was the case in the 2010 Wikileaks incident.[157]

***104** In April 2010, Wikileaks.org, a fringe website dedicated to publishing secret documents,[158] displayed a video of an American helicopter firing at civilians in Afghanistan.[159] This video was just the start; over the next few weeks Wikileaks published approximately 92,000 classified documents leaked to the website by an anonymous source within the IC,[160] later identified to be Army intelligence analyst Pfc. Bradley Manning. The Pentagon has frequently objected to

Wikileaks' policy of exposing national security secrets, saying "such information could be used by foreign intelligence services, terrorist groups and others to identify vulnerabilities, plan attacks and build new devices."[161] This level of unauthorized disclosure was unprecedented; Manning claimed to have trafficked 260,000 classified documents to Wikileaks.[162]

While arresting Manning was simple enough once he was identified, restoring national security by reclaiming the disclosed information was impossible.[163] Wikileaks refuses to return the ill-gotten documents and plans to continue publishing them.[164] This places the Pentagon in an undesirable position, as judicial injunctions are notoriously ineffective in curbing such behavior; shutting down one website leaves dozens of mirror sites free to operate abroad, beyond the reach of American courts.[165] The only safeguard that stops any interested party in obtaining information that could compromise the effectiveness of ongoing intelligence operations--not to mention the lives of those agents who depend on secrecy in the field--is the mere promise that Wikileaks will only release information it feels would not jeopardize national security operations.[166] From statements made by the New York Times and Wikileaks, it appears the leaked documents contain information that jeopardizes the safety of field operatives and could harm national security.[167] Instead of such information being in the hands of the intelligence committees who are knowledgeable and specialized in handling this sort of disclosure, it is in the hands of five untrained civilian volunteers ***105** who have stated that the goal is to use the information because they "enjoy crushing [the] bastards."[168]

The result of this leak underscores the importance of providing whistle-blowers with effective protection. Had Manning made his disclosures pursuant to the ICWPA procedures, the information he transferred would have been kept secure and gone directly into the hands of congressional intelligence committees, the legislative policymakers best suited to make meaningful changes in the IC when the Executive refuses to take action.[169] Had he done so, his agency would have been prohibited from retaliating against him because he would have done nothing wrong.[170] Even going to the IG would have been a safer alternative, as his disclosure would have been protected by statutory guarantees against agency retaliation.[171] Admittedly, he could have lost his security clearance in retaliation, but at least he could appeal that revocation within his agency.[172] By taking matters into his own hands and leaking information directly to the news media, Manning forfeited all protections available to him and now faces criminal charges.[173] Furthermore, the information he disclosed is now in unsafe hands, potentially accessible to every person in the world with an Internet connection. The only safeguards left are the promises of inexperienced civilians that they will redact what they deem to be sensitive information.[174] However, it is unlikely that these civilians will choose to redact much, as an increased volume of revealed information is more likely to provoke an investigation, which is their desired outcome.[175] Those who depend on secrecy to survive never agreed to have such individuals decide what is safe for disclosure and what is not.

B. Disadvantages of Increasing Whistle-Blower Protections

Though increased whistle-blower protection has unmistakable benefits, it must be conceded that protecting whistle-blowers has costs that must be considered as well.

***106 1. Calculable Costs**

The first and most obvious cost is that whistle-blower protections require enforcement, and any enforcement effort requires funding. The proposal in S. 372, for example, will require additional salaries for ICWPB members[176] and facilities in which to conduct business.[177] Presumably, a support staff will be required to support the work of the new board, and agency workload in prosecuting these cases will increase as they need to prepare cases for a whole new level of review. As far as expenses can be calculated, the Congressional Budget Office (CBO) estimated the cost of the implementing the ICWPB will cost $3 million annually.[178]

To evaluate if this cost is worth accepting, we must estimate the amount of money that whistle-blowing can save the IC. Quantifying the amount of theft, waste, or abuse in any government agency is difficult, especially when the agency is notoriously opaque, as the IC agencies are known to be. However, at least one scholar has estimated that approximately 10% of the general federal budget is lost to theft, waste, and abuse every year.[179] That scholar investigated portions of the federal government where the FCA was available to whistle-blowers to help control abuse of government resources and described the FCA as the most effective means for combating waste and abuse within agencies.[180] It would seem to follow that because the FCA is not available to IC whistle-blowers, the loss from waste, fraud, and abuse in the IC will likely exceed the 10% estimate.[181] For argument's sake, we will use the conservative 10% estimate of the $75 billion annual IC budget and conclude that the IC loses $7.5 billion each year from theft, waste, or abuse.

To put this in perspective, an additional level of protection against agency wrongdoing could be implemented for a mere fraction of a percent of the estimated $7.5 billion annual loss from unscrupulous behavior.[182] Put another way, the cost of implementing the ICWPB is 2,500 times less than the cost of theft, waste, and abuse in the IC.[183]

However, it is important not to be misled here. The creation of the ICWPB will not eliminate all occurrences of theft, waste, or abuse in the IC. It will only make it more likely that an IC whistle-blower will feel ***107** comfortable in exposing such occurrences because he will be able to seek meaningful review of retaliatory action taken against him. Although the amount saved under the ICWPB will not cancel out the entire annual loss to the IC from theft, waste, or abuse, the savings under the ICWPB will almost certainly exceed the amount saved under the current whistle-blowing scheme.

More important than the dollar amount of actual theft, waste, and abuse detected and saved is the dollar amount that will not occur in the first place once IC employees are empowered to become

successful whistleblowers. The IC would no longer have a reputation of being well-funded, yet unmanageable because any rank-and-file employee could potentially report on unscrupulousness. Therefore, theft, waste, and abuse in the IC would drop from its current level to a conceivably much lower level, as such dishonest actors move to easier targets to defraud.

2. Costs Due to Improperly Disclosed National Security Information

Thus far it has been estimated that the total cost of the ICWPB would be $3 million annually. However, in preparing this estimate, the CBO did not include the risk of increased accidental disclosures of information related to national security. Such risks can be of incalculable cost because, as the Pentagon noted, information related to national security can be used "by foreign intelligence services, terrorist groups and others to identify vulnerabilities, plan attacks and build new devices."[184] The risk of improper disclosure increases whenever information is entrusted to more individuals, which would occur as the complaint advances through additional layers of review. The risk increases because any individual may make disclosures to America's enemies either accidently, or, as in the case of spies or vigilante whistle-blowers, on purpose. Hence, controlling the information's security becomes increasingly difficult. As discussed in Part I.A.1, the cost of exposure is steep and can include embarrassment, ineffective intelligence operations, and even the deaths of agents in the field. Therefore, there is a strong argument for keeping information in as few hands as possible.

However, this argument does not foreclose the prudence of reform, and in fact may strengthen it. There will always be whistle-blowers who feel that they must do what is right and make disclosures to save lives or combat corruption, even when they have no legal means to do so. The Wikileaks incident showed how much damage a single whistle-blower of that ilk can cause and how quickly intelligence information can spread into so many hands. However, by increasing protections, it makes it less likely that such individuals will choose that route if an effective legal alternative exists. Therefore, by increasing whistle-blower protections, for instance, by ***108** providing an additional layer of review through creating the more approachable and neutral ICWPB, the government reduces the number of hands into which information related to national security is placed.

V. Suggestions for Improvement

As good a start as the ICWPB is, it is only a start. Two major problems still remain: (1) the ICWPB's location within the Executive Branch; and (2) the lack of proper incentives for IC whistle-blowers to report instances of theft, waste, and abuse.

The first problem can be corrected simply by making ICWPB decisions reviewable by the Federal Circuit. While this suggestion runs afoul of the Supreme Court's decision in Egan, its adoption is

critical because review outside of the Executive Branch is necessary to prevent agency wrongdoing.[185] This suggestion is gaining greater acceptance, as evidenced by a recent MSPB decision that indicated a willingness to at least limit the reach of Egan. In Conyer v. DOD,[186] the MSPB held that Egan's prohibition against MSPB review of adverse personnel actions related to security clearances was inapplicable to positions designated as "sensitive" because such a designation merely indicated a relation to national security and trustworthiness, but did not grant access to classified information.[187] The MSPB reasoned that "any matter in which the government [merely] asserts a national security interest" cannot be free from judicial review unless a security clearance is at stake because it would "without any Congressional mandate or imprimatur, preclude Board and judicial review of alleged unlawful discrimination, whistle-blower retaliation, and a whole host of other constitutional and statutory violations for multitudes of federal employees subjected to otherwise appealable removals and other adverse actions."[188] While this single decision does not disturb Egan as it relates to security clearance revocations, Conyer may be evidence that in the future it will become less likely that the Executive can assert Commander-in-Chief privilege to evade judicial review. The next steps, like opening the ICWPB to Federal Circuit review, may not be far behind.

Furthermore, the ICWPB should be empowered to hear qui tam complaints from IC whistle-blowers and offer them a percentage of the waste saved, much like the FCA provides for relators.[189] The IGs are already authorized ***109** to give awards to IC relators under federal statute, so the suggestion should not be foreign to the Executive Branch.[190] Pursuant to 5 U.S.C. § 4512, an agency's IG may give the lesser of $10,000 or 1% of agency savings to any employee who disclosed instances of fraud, waste, or abuse.[191] However, instead of capping the amount at $10,000, the award should be set to the maximum award possible from the ICWPB, currently fixed at $300,000.[192] Currently, the ICWPB can only award an amount sufficient "to return the employee . . . as nearly as practicable and reasonable, to the position such employee . . . would have held had the violation not occurred."[193] Therefore, the whistle-blower is not incentivized to bring cases, but rather merely reimbursed if he was improperly punished for doing so.

The reason for adding the qui tam capability is simple and straightforward. First, it would authorize the ICWPB to hear complaints from those not yet injured by retaliatory action. The ICWPB is the logical organization to hear such complaints because it is already staffed by individuals (presidential appointees, agency heads and IGs) who are: (1) authorized to hear classified information; (2) knowledgeable about the business of the IC; and (3) charged with rooting out instances of theft, waste, and abuse. Furthermore, the ICWPB would be perceived as a more impartial fact finding body than the intra-agency reviews currently available because of the ICWPB's recusal requirement. Additionally, the ability to recover in excess of the injury suffered by the relator whistle-blower would be the key requirement in transforming rank-and-file employees into a policing mechanism for the IC. Without giving a whistle-blower the ability to profit from his actions, the upgraded ICWPB will only attract those IC workers who would likely have done the right thing anyway. In an environment where agency management cannot effectively prevent waste on its own or where such instances will be subtle or difficult to detect,

mere job protection is insufficient to motivate the average federal employee to take the time to root out wrongdoing, as he is required to do under Executive Order 12674. Even if Congress could guarantee that no whistle-blower will ever be retaliated against, there would still be a less than optimum level of whistle-blowing because whistle-blowers may not care to get bogged down in the courts when there is no incentive for them to blow the whistle in the first place. Furthermore, this new opportunity to obtain compensation for successful whistle-blowing would entice those workers who currently do not care enough to take action or prefer to look the other way. Therefore, empowering ***110** the ICWPB to offer monetary incentives is one of the only ways that IC whistle-blowers will take up the extra work to hold their agencies responsible for wrongdoing. Moreover, the monetary incentive should be allowed to exceed $10,000 because waste in the IC can reach at least $7.5 billion per year. The amount awarded for successful whistle-blowing should more accurately reflect the social benefit derived from such activity in order to encourage a socially optimum level of whistle-blowing.[194]

An added benefit of authorizing the IC to use the ICWPB to bring qui tam actions is that it eliminates the need to resolve the current circuit split as to whether Congress intended the current version of the FCA to allow government relators.[195] If new legislation explicitly empowers the ICWPB to have jurisdiction over such cases, then there would be no such confusion frustrating the work of IC whistle-blowers, who by their nature must be government relators.

Some scholars have argued that extending this incentive to government workers creates a conflict of interest.[196] As one such scholar explained, it creates an incentive for a government relator who discovers an instance of theft, waste, or abuse to ignore it and even encourage it to grow until it becomes profitable for him to initiate a private lawsuit for personal gain.[197] Thus, theft, waste, and abuse are actually amplified by providing incentives. Though this is a troubling risk, the alternative is to stay the course and let all theft, waste, and abuse continue largely unchecked in the expansive IC bureaucracy, which can barely manage its work product, much less audit itself on every suspicion of waste.[198]

Incentivizing intelligence workers is perhaps the only way to effectively ferret out theft, waste, and abuse. Under the FCA, even if government workers could not be relators, at least a private citizen could.[199] In the IC, where information related to theft, waste, and abuse is likely to be intertwined with classified information, only government workers with security clearances would ever be able to learn of the wrongful conduct. Therefore, by denying IC workers an incentive to blow the whistle, the IC will become ***111** uniquely immune to examination by motivated, self-interested whistleblowers, and therefore will attract unscrupulous individuals.

Conclusion

The Executive oversees the IC more so than any other federal agencies. Its employees work under a virtual gag order and Congress is kept at arm's length from its day-to-day operations. As the IC

expands, opportunities for theft, waste, and abuse multiply while the IC's ability to self-police deteriorates. Congress should act now to create a new forum where IC whistle-blowers can seek meaningful review outside of retaliatory security clearance revocations and other prohibited personnel practices--a place where they will have the opportunity to be heard outside of their own agency. The ICWPB can provide a framework, which can later be upgraded to enable review outside of the Executive Branch, that would finally end the Executive's hegemony over the critical issue of information related to national security. Also utilizing this forum, eventual additional legislation can give intelligence workers an opportunity to speak and a place to pursue qui tam actions, which would provide a financial incentive for IC whistle-blowers to do the right thing and potentially save the government billions of dollars.

The ICWPB is an important step in the right direction that makes possible real protection for IC whistle-blowers and lays the groundwork for them to overcome the social stigma of whistle-blowing. The IC is vulnerable to fraud, largely free from congressional oversight, and in need of strong, empowered, motivated whistle-blowers. The ICWPB can help the IC rise above the corruption that drains its resources and effectiveness and allow it to focus on its mission of protecting America.

Footnotes

a1 J.D. Candidate, George Mason University School of Law, 2013. I am grateful to Professor Nathan Sales and the members of the Journal of Law, Economics & Policy for their support and assistance.

1 National Security Whistleblowers in the Post-September 11th Era: Lost in a Labyrinth and Facing Subtle Retaliation: Hearing Before the Subcomm. on Nat'l Sec., Emerging Threats, and Int'l Relations of the Comm. on Gov't Reform, 109th Cong. 125 (2006) (statement of Lt. Col. Anthony Shaffer) [hereinafter Lost in a Labyrinth].

2 Id. at 126.

3 Id. at 127.

4 Id. at 125.

5 See infra Part I.B.2 for a discussion on the Intelligence Community Whistleblower Protection Act, which provides this pathway to Congress for concerned whistle-blowers.

6 Lost in a Labyrinth, supra note 1, at 128.

7 Id. at 128-29.

8 See infra Part II for a discussion of security clearance retaliation and why it is not subject to meaningful review.

9 Lost in a Labyrinth, supra note 1, at 125.

10 See infra Part III.A.2 for a discussion on the dangers of such vigilante whistle-blowing and the recent Wikileaks incident.

11 Whistleblower Protection Enhancement Act of 2009 (WPEA), S. 372, 111th Cong. (2009); Bill Summary & Status: 111th Congress (2009-2010) S. 372, LIBRARY OF CONGRESS THOMAS, http:// hdl.loc.gov/loc.uscongress/legislation.111s372: (last visited Nov. 6 2011).

12 S. 372, officially titled the "Whistleblower Protection Enhancement Act of 2009," contains many provisions besides the creation of the Intelligence Community Whistleblower Protection Board that are well-covered by existing scholarship. See, e.g., Jocelyn Patricia Bond, Efficiency Considerations and the Use of Taxpayer Resources: An Analysis of Proposed Whistleblower Protection Act Revisions, 19 FED. CIR. B.J. 107 (2009). However, existing scholarship has not examined the portions of the bill that would create the Board. This paper limits its consideration to these unvisited provisions.

13 See infra Part I.B.3 for the powers of the ICWPB.

14 See infra Part IV for suggestions as to how the ICWPB can be upgraded to properly incentivize whistle-blowers.

15 The current intelligence agencies include, among others, the Defense Intelligence Agency (DIA), the Central Intelligence Agency (CIA), the National Security Agency (NSA), and the intelligence elements within the Department of Defense, the Department of State, the Army, Navy, Air Force and Marine Corps, the Department of the Treasury and the Federal Bureau of Investigation. Exec. Order No. 12,333, 46 Fed. Reg. 59,941, 59,953 (Dec. 8, 1981). The list of intelligence agencies grows either by Congressional inclusion into statutes or by Presidential designation. Czarkowski v. MSPB, 390 F.3d 1347, 1350 (Fed. Cir. 2004).

16 See Office of the Dir. of Nat'l Intelligence, Overview of the Intelligence Community for the 111th Congress (2010), available at http:// www.dni.gov/overview.pdf.

17 Executive Order 12,968 recognizes that information classified in the interest of national security "can cause irreparable damage to the national security and loss of human life." Exec. Order No. 12,968, 60 Fed. Reg. 40,245, 40,245 (Aug. 2, 1995).

18 For the sake of preventing confusion, this paper uses the terms "theft, waste, and abuse" to include all manner of protected disclosures. Individual legislation controls the ultimate scope of protected disclosures, and their language as to what constitutes theft, waste, and abuse differs slightly, but not meaningfully. For example, the Inspector General Act of 1978 labels disclosures that trigger whistle-blower protections as "activity constituting a violation of law, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority or a substantial and specific danger to the public health and safety," where the Whistleblower Protection Act instead refers to disclosures of "(i) a violation of any law, rule, or regulation, or (ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety." Whistleblower Protection Act of 1989, 5 U.S.C. § 2302(b)(8)(i)-(ii) (2010); Inspector General Act of 1978, 5 U.S.C. app. § 7(a) (2007). For our purposes, the definition of protected disclosures will be simplified to those relating to "theft, waste, and abuse."

19 Lt. Col. Anthony Shaffer's discovery of DIA mismanagement, discussed supra text accompanying note 3, at 1, would be an example

of such a discovery.

20 Executive Order 12,968 requires that access to information related to national security can only be given to those with a demonstrated need to know of it, and that only an agency head can make such a determination, not an employee-whistle-blower. Exec. Order No. 12,968, 60 Fed. Reg. 40,245, 40,246 (1995).

21 U.S. CONST. art. II, § 1.

22 U.S. CONST. art. II, § 2, cl. 1.

23 Nathan Alexander Sales, Secrecy and National Security Investigations, 58 ALA. L. REV. 811, 821 (2007).

24 Id. at 818-19.

25 Id. at 819.

26 Id. at 820.

27 See infra Part II.B.2 for a discussion of this legislation and how it relates to the executive/legislative contest over information related to national security.

28 Statement on Signing the Intelligence Authorization Act for Fiscal Year 1999, 2 PUB. PAPERS 1825, 1825 (Oct. 20, 1998).

29 Id.

30 S. 372 -- The Whistleblower Protection Enhancement Act of 2009, Before the Subcomm. on Oversight of Gov't Managment, the Fed. Workforce, and D.C., U.S. Senate 11 (2009) (statement of Rajesh De, Deputy Assistant Att'y Gen.), available at http://www.justice.gov/olp/pdf/rajeshdewhistleblower-senate.pdf.

31 Id. at 10.

32 See Exec. Order No. 12,968, 60 Fed. Reg. 40,245, 40,246, 40,252, 40,254 (Aug. 7, 1995).

33 CIA v. Sims, 471 U.S. 159 (1985).

34 Id. at 172, 175.

35 While an extensive study of the evolution of this need for secrecy is beyond the scope of this paper, it is sufficient to conclude that the need for secrecy in national security matters is well accepted by American courts. For an excellent piece tracing the developments through judicial decisions, see Sales, supra note 23, at 818-65.

36 Dep't of the Navy v. Egan, 484 U.S. 518, 518-34 (1988).

37 Id. at 521.

38 Id. at 521-22.

39 Id.

40 Id. at 527-28.

41 Id. at 529-30.

42 Egan, 484 U.S. at 527.

43 Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, § 701(b), 112 Stat. 2396, 2413-14 (1998) (codified at 5 U.S.C. app. § 8H (2007)).

44 See, e.g., Louis Fisher, Cong. Research Serv., RL 33215, National Security Whistleblowers 2-5 (2005), available at http://www.lexisnexis.com.mutex.gmu.edu/congcomp/getdoc?CRDC-ID=CRS-2005-GVF-0663 (last accessed August 31, 2010).

45 Id. at 3-4.

46 Id. at 2-3.

47 Id.

48 Id. at 3-4.

49 Id.

50 Lloyd-LaFollette Act of 1912, Pub. L. No. 62-336, § 6, 37 Stat. 539, 555 (1912).

51 Exec. Order No. 12,968, 60 Fed. Reg. 40,245, 40,246 (Aug. 2, 1995).

52 Id.

53 See Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, § 701(b) 112 Stat. 2396, 2413-14 (1998) (codified at 5 U.S.C. app. § 8H (2007)).

54 Id.

55 Statement on Signing the Intelligence Authorization Act for Fiscal Year 1999, 2 PUB. PAPERS 1825 (Oct. 20, 1998).

56 See id. § 702, 112 Stat. at 2413-16.

57 Whistleblower Protection Act of 1989, 5 U.S.C. § 2302(a)(2)(C)(ii) (2006).

58 False Claims Act, 31 U.S.C. § 3730(d) (2006). See also infra Part IV for a discussion of why the FCA is not available to IC workers.

59 Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, § 702, 112 Stat. 2396 (1998) (codified at 5 U.S.C. app. § 8H (2007)); Inspector General Act of 1978, Pub. L. No. 95-452, 92 Stat. 1101 (codified as amended at 5 U.S.C. app. §§ 1-12 (2007)).

60 5 U.S.C. app. §§ 1-12 (2007).

61 Id. § 3(a).

62 Id. § 2(2)-(3).

63 Specifically, the statute allows the IG to hear and investigate complaints of the "possible existence of an activity constituting a violation of law, rules, or regulations, or mismanagement, gross waste of funds, abuse of authority or a substantial and specific danger to the public health and safety." Id. § 7(a).

64 Id. § 7(c).

65 Inspector General Act of 1978, Pub. L. No. 95-452, 92 Stat. 1101 (codified as amended at 5 U.S.C. app. § 3(b) (2007)).

66 Id. §§ 3(a), § 8H(a)(1).

67 This was true before the ICWPA. The next section will detail how this scenario has changed.

68 Inspector General Act of 1978, 5 U.S.C. app. § 5(e) (2007).

69 The IG would make the disclosure to the agency head and Congress by including it in his annual or periodic reports to Congress. Id. § 5.

70 The Inspector General Act does not require reporting on the number of complaints made but found not to be credible. Id. § 5.

71 See Id. § 5(b)-(d) (requiring the Inspectors General to make periodical, statistics-based reports to the agency heads for transmittal to Congress, and compelling them to immediately make a detailed report if they believe the information concerns to be "particularly serious or flagrant problems . . . .").

72 Intelligence Community Whistleblower Protection Act of 1998, Pub. L. No. 105-272, § 702, 112 Stat. 2396 (1998) (codified at 5 U.S.C. app. § 8H (2007)).

73 Id. § 8H.

74 Id. § 8H(a)-(b).

75 Id. § 8H(c).

76 Id. § 8H(d).

77 Lost in a Labyrinth, supra note 1, at 1-4.

78 Id. at 5-6 (statement of Rep. Henry Waxman).

79 Id. at 122-32 (statement of Lt. Col. Anthony Shaffer).

80 Id. at 132-42 (statement of Michael German, former Special Agent, Fed. Bureau of Investigation).

81 Id. at 135-36.

82 Id. at 136-39.

83 Lost in a Labyrinth, supra note 1, at 136-37 (statement of Michael German, Former Special Agent, Fed. Bureau of Investigation).

84 H.R. 1507, 111th Cong. (2009); S. 372, 111th Cong. (2009).

85 Id. § 10 (amending 5 U.S.C. § 2302, adding § 2303A(a)(1)-(2)).

86 Id. (amending 5 U.S.C. § 2302, adding § 2303A(c)(4)).

87 The MSPB describes itself as a "quasi-judicial agency in the Executive branch that serves as the guardian of Federal merit systems." It accomplishes this role by adjudicating appeals by individual federal employees, as well as studying the merits system. MERIT SYS. PROT. BD., About MSPB, http://www.mspb.gov/About/about.htm (last visited Jan. 15, 2011).

88 H.R. 1507, 111th Cong. § 14 (2009) (amending 5 U.S.C. § 77, adding § 7702A).

89 S. 372, 111th Cong. § 201 (2009) (amending 50 U.S.C. § 402, adding § 120).

90 Id. § 201 (adding § 120(a)-(b)).

91 Id. § 201 (amending 50 U.S.C. § 402, adding § 120(b)).

92 Id.

93 Id.

94 Id.

95 S. 372, 111th Cong. § 201 (2009) (adding § 121(c)).

96 Id. (adding § 121(c)(4)).

97 Id. (adding § 121(c)(5)(A)(i)-(ii)).

98 Id. (adding §§ 121(c)(2), 121(c)(4)(E)).

99 Id.

100 Id. (amending 50 U.S.C. § 402, adding § 121(c)(4)(E)).

101 Whistleblower Protection Enhancement Act of 2009, S. 372, 111th Cong. § 202 (as reported by S. Comm. on Homeland Sec. and Governmental Affairs, Dec. 3, 2009) (amending 50 U.S.C. § 435B(b), adding § 3001(j)(3)-(4)).

102 Id. (amending 50 U.S.C. § 435B(b), adding § 3001(j)(5)).

103 Id. (amending 50 U.S.C. § 435B(b), adding § 3001(j)(4)(F)).

104 Id. (amending 50 U.S.C. § 435B(b), adding § 3001(j)(4)(G)).

105 Exec. Order No. 12674, 54 Fed. Reg. 15159, 15159 (1989).

106 Id.

107 See, e.g., Lost in a Labyrinth, supra note 1, at 130-31 (statement of Lt. Col. Anthony Shaffer) (who felt there was no place, including the office of the IG, to seek meaningful review of his retaliatory security clearance determination); see also id. at 135-37 (statement of Michael German, Former Special Agent, Fed. Bureau of Investigation) (who tried to coax his agency's IG into protecting him from a malicious investigation made in retaliation for his protected disclosures).

108 Inspector General Act of 1978, 5 U.S.C. app. § 3(a) (2007).

109 Id. § 3(a)-(b).

110 Id. § 3.

111 Pamela S. Karlan, Lessons Learned: Voting Rights and the Bush Administration, 4 Duke J. Const. L. & Pub. Pol'y 17, 28 (2009).

112 See, e.g., U.S. Dep't of Justice Office of the Inspector Gen. & Office of Prof'l Responsibility, an Investigation Into the Removal of Nine U.S. Attorneys in 2006 56-59 (2008), available at http:// www.usdoj.gov/oig/special/s0809a/final.pdf (finding that the conduct of key, high level presidential appointees severely damaged public confidence in the Justice Department due to their unfair, arbitrary and "fundamentally flawed" removal decisions); see also Karlan, supra note 110, at 28.

113 Karlan, supra note 111.

114 Lost in a Labyrinth, supra note 1, at 135-37 (statement of Michael German, Former Special Agent, Fed. Bureau of Investigation).

115 Id.

116 Id. at 374-422.

117 Id. at 4 (statement of Rep. Christopher Shays).

118 Id. at 374-422.

119 Id. at 41.

120 Lost in a Labyrinth, supra note 1, at 412-13 (statement of Inspector Gen. Gregory Friedman, U.S. Dep't of Energy).

121 Id.

122 Id. at 410.

123 Id. at 406 (statement of Inspector Gen. Glenn Fine, U.S. Dep't of Justice).

124 Id. at 132-42 (statement of Michael German, Former FBI Special Agent).

125 Id. at 405 (statement of Inspector Gen. Glenn Fine, U.S. Dep't of Justice).

126 Lost in a Labyrinth, supra note 1, at 127 (statement of Lt. Col. Anthony Shaffer).

127 Dep't of the Navy v. Egan, 484 U.S. 518, 527 (1988).

128 Lost in a Labyrinth, supra note 1, at 128-29 (statement of Lt. Col. Anthony Shaffer).

129 See, e.g., Dep't of Justice, Statement of Rajesh De, supra note 30, at 8.

130 Id. at 7-8.

131 Exec. Order 12968, 60 Fed. Reg. 40,245, 40,252 (1995).

132 Id. at 40,252-53.

133 Id.

134 Dep't of Justice, Statement of Rajesh De, supra note 30, at 7.

135 H.R. 1507 § 10(c)(3), 111th Cong. (2009) (amending 5 U.S.C. § 2302, adding § 2302A(c)(4)).

136 See U.S. CONST. art. III §§ 1-2 (providing life tenure for judges and assigning the Supreme Court appellate jurisdiction over the inferior federal courts).

137 H.R. 1507 § 10, 111th Cong. (2009) (amending 5 U.S.C. § 2302, adding § 2302A(c)(4)).

138 Dep't of the Navy v. Egan, 484 U.S. 518, 527 (1988); H.R. 1507 § 14(b)(1), 111th Cong. (2009) (amending 5 U.S.C. § 77, adding § 7702A).

139 Lost in a Labyrinth, supra note 1, at 6 (statement of Rajesh De, Deputy Assistant Att'y Gen., Office of Legal Policy, Dep't of Justice).

140 S. 372 § 201, 111th Cong. (2009).

141 S. 372 § 201, 111th Cong. (2009) (amending 50 U.S.C. § 402, adding § 120).

142 Inspector General Act of 1978, 5 U.S.C. app. § 3 (2007).

143 Exec. Order No. 12968, 60 Fed. Reg. 40245, 40252-54 (Aug. 7, 1995); S. 372 § 201, 111th Cong. (2009) (amending 50 U.S.C. § 402, adding § 120(b)).

144 False Claims Act Correction Act (S. 2041): Strengthening the Government's Most Effective Tool Against Fraud for the 21st Century, Hearing Before the S. Comm. on the Judiciary, 110th Cong. 1 (2008) (statement of Sen. Leahy, Chairman, S. Comm. on the Judiciary), available at http:// frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_senate_hearings&docid=f:42809.wais.pdf (last accessed September 15, 2010). See also Barry M. Landry, Note, Deterring Fraud to Increase Public Confidence: Why Congress Should Allow Government Employees to File Qui Tam Lawsuits, 94 Minn. L. Rev. 1239, 1241 (2010) (explaining that the FCA is the most effective tool because it gives the qui tam relator a monetary reason to come forward).

145 Dana Priest & William M. Arkin, Top Secret America: A Hidden World, Growing Beyond Control, Wash. Post, July 19, 2010, at A1.

146 Id.

147 Id.

148 Id.

149 Id.

150 Id.

151 Priest & Arkin, supra note 145.

152 Id.

153 Id.

154 Lost in a Labyrinth, supra note 1 (statement of Lt. Col. Anthony Shaffer).

155 See, e.g., id. (statement of Lt. Col. Anthony Shaffer) (describing his agency's culture of abhorrent values, self-preservation and fear of retaliation).

156 For example, an IG is authorized to give up to $10,000 to a whistle-blower in exchange for his money-saving disclosure. 5 U.S.C. § 4512(a) (2010).

157 Elizabeth Newell, Backing Up Whistleblowers, GovernmentExecutive.com (Feb. 2, 2011), http://www.govexec.com/dailyfed/0211/020211mm.htm.

158 Stephanie Strom, Pentagon Sees a Threat From Online Muckrakers, N.Y. Times, Mar. 18, 2010, at A18.

159 Noam Cohen & Brian Stelter, Airstrike Video Brings Attention to Whistle-Blower Site, N.Y. Times, Apr. 7, 2010, at A8.

160 Eric Schmitt & Helene Cooper, Document Leak Adds to Pressure on White House, N.Y. Times, July 27, 2010, at A1.

161 Strom, supra note 158.

162 Elisabeth Bumiller, Army Leak Suspect Is Turned In, by Ex-Hacker, N.Y. Times, June 8, 2010, at A1.

163 See Eric Schmitt, In Disclosing Secret Documents, WikiLeaks Seeks 'Transparency,' N.Y. Times, July 26, 2010, at A11.

164 Thom Shanker, WikiLeaks and Pentagon Disagree About Talks, N.Y. Times, Aug. 19, 2010, at A10.

165 Cohen & Stelter, supra note 159.

166 See Schmitt & Cooper, supra note 160.

167 See id.

168 Id.; Cohen & Stelter, supra note 159.

169 5 U.S.C. app. § 8H(d) (2007).

170 See H.R. 1507 § 10, 111th Cong. (2009) (amending 5 U.S.C. § 2302, adding § 2303A(a)(1)-(2)).

171 See 5 U.S.C. app. § 7(c) (2007).

172 Exec. Order No. 12,968, 60 Fed. Reg. 40,245, 40,252 (Aug. 2, 1995).

173 See 5 U.S.C. app. §§ 8H(a), (d) (2011).

174 Schmitt & Cooper, supra note 160.

175 Id.

176 S. 372, 111th Cong. § 201 (2009) (amending 50 U.S.C. § 402, adding § 120(b)(4)).

177 Id. (amending 50 U.S.C. § 402, adding § 120(c)).

178 Cong. Budget Office, Cost Estimate, S. 372: Whistleblower Protection Enhancement Act of 2009 (2009), available at http://www.govtrack.us./data/us/111/bills.cbo/s372.pdf.

179 Landry, supra note 144, at 1239-40 n.3.

180 Id. at 1241-42.

181 See infra Part IV for a discussion of why the FCA is not available to IC workers.

182 This is calculated by dividing the cost of the ICWPB by the loss estimated at 10% of the IC budget of $75 billion, or (3,000,000 / 7,500,000,000) = .0004.

183 This is calculated by inverting the earlier value of .0004.

184 Strom, supra note 158.

185 Dep't of the Navy v. Egan, 484 U.S. 518 (1988).

186 Conyer v. U.S. Dep't of Defense, 2010 M.S.P.B. 247 (2010).

187 Id. at ¶¶ 13, 16.

188 Id. at ¶¶ 16-24.

189 The FCA permits plaintiffs to come forward who are not actually themselves injured by the fraud, but to proceed qui tam (that is, on behalf of the government) and share a percentage of the recovery. See False Claims Act, 31 U.S.C. § 3730(c)-(d) (2009). Here, the ICWPB would hear cases by individuals having knowledge of instances of theft, waste, and abuse but who are not themselves victims

of it.

190 5 U.S.C. § 4512(a).

191 Id.

192 S. 372, 111th Cong. § 202 (2009) (amending 50 U.S.C. § 435B(b), adding § 3001(j)(4)(B)).

193 Id.

194 See supra Part III.B.1, for how this figure was calculated.

195 Compare United States ex rel. Leblanc v. Raytheon, 913 F.2d 17, 20 (1st Cir. 1990) (holding that government relators who are required to disclose fraud as a part of their job cannot bring FCA actions as original sources of the disclosure), and Exec. Order No. 12,674, 54 Fed. Reg. 15,159, 15,159 (Apr. 12, 1989) (requiring all federal employees to uncover and report instances of fraud), with United States ex rel. Williams v. NEC Corp., 931 F.2d 1493, 1501 (11th Cir. 1991) (holding that government employee relators are not barred from being original sources merely because they are required to uncover fraud as a condition of their employment). See also Joan R. Bullock, The Pebble in the Shoe: Making the Case for the Government Employee, 60 TENN. L. REV. 365 (1993) (discussing generally this circuit split and the rationales behind it).

196 Bullock, supra note 195, at 382-83, 387.

197 Id. at 382-83.

198 Priest & Arkin, supra note 145.

199 False Claims Act, 31 U.S.C. § 3730(b)(1) (2010).

MODEL AGENCY NOTICE TO EMPLOYEES AND CONTRACTORS
CONCERNING SAFEGUARDING OF CLASSIFIED INFORMATION
AND USE OF GOVERNMENT INFORMATION TECHNOLOGY SYSTEMS

The recent disclosure of U.S. Government documents by WikiLeaks has resulted in damage to our national security. Each federal employee and contractor is obligated to protect classified information pursuant to all applicable laws, and to use government information technology systems in accordance with agency procedures so that the integrity of such systems is not compromised.

Unauthorized disclosures of classified documents (whether in print, on a blog, or on websites) do not alter the documents' classified status or automatically result in declassification of the documents. To the contrary, *classified information, whether or not already posted on public websites or disclosed to the media, remains classified, and must be treated as such by federal employees and contractors, until it is declassified by an appropriate U.S. Government authority*.[1]

Federal employees and contractors therefore are reminded of the following obligations with respect to the treatment of classified information and the use of non-classified government information technology systems:

- Except as authorized by their agencies and pursuant to agency procedures, federal employees or contractors shall not, while using computers or other devices (such as Blackberries or Smart Phones) that access the web on non-classified government systems, access documents that are marked classified (including classified documents publicly available on the WikiLeaks and other websites), as doing so risks that material still classified will be placed onto non-classified systems. This requirement applies to access that occurs either through agency or contractor computers, or through employees' or contractors' personally owned computers that access non-classified government systems. This requirement does not restrict employee or contractor access to non-classified, publicly available news reports (and other non-classified material) that may in turn discuss classified material, as distinguished from access to underlying

[1] Executive Order 13526, *Classified National Security Information* (December 29, 2009), Section 1.1.(c) states, "Classified Information shall not be declassified automatically as a result of any unauthorized disclosure of identical or similar information."

documents that themselves are marked classified (including if the underlying classified documents are available on public websites or otherwise in the public domain).

- Federal employees or contractors shall not access classified material unless a favorable determination of the person's eligibility for access has been made by an agency head or the agency head's designee, the person has signed and approved non-disclosure agreement, the person has a need to know the information, and the person has received contemporaneous training on the proper safeguarding of classified information and on the criminal, civil, and administrative sanctions that may be imposed on an individual who fails to protect classified information from unauthorized disclosure.

- Classified information shall not be removed from official premises or disclosed without proper authorization.

- Federal employees and contractors who believe they may have inadvertently accessed or downloaded classified or sensitive information on computers that access the web via non-classified government systems, or without prior authorization, should contact their information security offices for assistance.

Thank you for your cooperation, and for your vigilance to these responsibilities.